

VA



U.S. Department
of Veterans Affairs
Office of Construction &
Facilities Management



Physical Security Design Manual

JANUARY 2015

For VA **Mission Critical Facilities**

**U.S. DEPARTMENT OF
VETERANS AFFAIRS**

**PHYSICAL SECURITY
DESIGN MANUAL**

FOR

**MISSION CRITICAL
FACILITIES**

JANUARY 2015

TABLE OF CONTENTS

1	INTRODUCTION	1
1.0	Purpose	1
1.1	Authority.....	1
1.2	VA Facilities.....	2
1.3	Introduction to Physical Security Concepts.....	4
1.4	Objectives of VA Physical Security Design	6
1.5	Requirements for Physical Security Subject Matter Specialists	6
1.6	Budgeting and Programming for Physical Security.....	7
1.7	Risk Assessment of VA Facilities.....	7
1.8	Document Distribution, Use, and Control.....	8
1.9	Administration and Enforcement	8
1.10	Interpretations and Exceptions.....	8
2	GLOSSARY & ACRONYMS.....	11
3	SITE CONSIDERATIONS	18
3.0	Scope, Purpose, and Goals	18
3.1	Standoff Distance	18
3.2	Perimeter Fences	18
3.3	Vehicle and Pedestrian Screening	19
3.4	Anti-ram Rated Vehicle Barriers	21
3.5	Parking	22
3.6	Site Lighting	24
4	BUILDING ENTRANCES & EXITS.....	27
4.0	Scope, Purpose, and Goals	27
4.1	Public Entrances and Lobbies	27
4.2	Patient Drop-offs.....	30
4.3	Building Exits and Life Safety Considerations	31
5	FUNCTIONAL AREAS.....	33
5.0	Scope, Purpose, and Goals	33

5.1	Agent Cashier.....	33
5.2	Caches	34
5.3	Childcare/Development Center.....	36
5.4	Main Computer Room.....	36
5.5	Emergency Department.....	37
5.6	Emergency and/or Standby Generator Room	39
5.7	Energy Center/Boiler Plant	40
5.8	Fire Command Center (FCC)	41
5.9	Incident Command Center.....	41
5.10	Loading Dock and Service Entrances.....	42
5.11	Mailroom	45
5.12	Pharmacy.....	46
5.13	Police Operations Room and Holding Room	48
5.14	Records Storage and Archives.....	50
5.15	Research Laboratory and Vivarium.....	50
5.16	Security Control Center	54
6	BUILDING ENVELOPE.....	59
6.0	Scope, Purpose, and Goals	59
6.1	Walls	59
6.2	Fenestration and Doors.....	60
6.3	Atria	61
6.4	Roofs	62
6.5	Air Intakes and Exhausts Servicing Critical Equipment.....	63
6.6	Calculation Methods.....	64
7	STRUCTURAL SYSTEM.....	65
7.0	Scope, Purpose, and Goals	65
7.1	Blast Resistance	66
7.2	Progressive Collapse.....	67
7.3	Column Protection	67
7.4	Wall Protection	68

7.5	Anti-ram Resistance	68
7.6	Calculation Methods.....	69
8	UTILITIES & BUILDING SERVICES	70
8.0	Scope, Purpose, and Goals	70
8.1	Utility Entrances	70
8.2	Site Distribution	71
8.3	Energy Center	73
8.4	Water and Fuel Storage	73
9	BUILDING SYSTEMS	79
9.0	Scope, Purpose, and Goals	79
9.1	HVAC systems	80
9.2	Electrical Systems	81
9.3	Telecommunications Systems.....	82
9.4	Plumbing Systems.....	86
9.5	Fire Protection Systems	86
10	SECURITY SYSTEMS.....	87
10.0	Scope, Purpose, and Goals	87
10.1	Electronic Security Systems.....	87
10.2	Physical Access Control System.....	88
10.3	Intrusion Detection System.....	89
10.4	Video Assessment and Surveillance.....	92
10.5	Duress, Security Phones, and Intercom System	97
10.6	Detection and Screening Systems	101
11	REFERENCES.....	103

1 INTRODUCTION

1.0 Purpose

This Manual contains the *physical security* standards for improving the protection of mission critical facilities of the U.S. Department of Veterans Affairs (VA). Mission Critical facilities are those required to continue operation during a natural or manmade extreme event. Design and construction standards are provided for the physical security of new buildings, additions, and *major alterations*. In addition, standards are provided to improve the physical security for existing mission critical facilities.

The requirements of this manual are to be coordinated with all VA design and construction requirements for the *mitigation* of other hazards, such as *earthquake* and *hurricane*, in order to complete a multi-hazard approach to physical security planning, design, and construction. In addition, it is intended that the requirements of this manual be coordinated with the requirements of the Life Safety Code, NFPA 101.

1.1 Authority

It has long been the policy of the United States to assure the continuity and viability of mission critical infrastructure. Executive Order 12656, issued November 18, 1988, states, "The head of each Federal department and agency shall be prepared to respond adequately to all national security emergencies." Furthermore, the "head of each Federal department and agency shall ensure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities." The Order also requires that the "head of each Federal department and agency shall: identify facilities and resources, both government and private, essential to the national defense and national welfare, and assess their vulnerabilities and develop strategies, plans, and programs to provide for the security of such facilities and resources, and to avoid or minimize disruptions of essential services during any national security emergency."

Public Law 107-188, Public Health Security and Bioterrorism Preparedness and Response Act of 2002 enacted June 12, 2002, requires actions to enhance the readiness of Department of Veterans Affairs medical centers to enable them to fulfill their obligations as part of the Federal response to public health emergencies. Under section 154 the law specifically requires that the "Secretary of Veterans Affairs shall take appropriate actions to enhance the readiness of Department of Veterans Affairs medical centers to protect the patients and staff of such centers from chemical or biological attack or otherwise to respond to such an attack and so as to enable such centers to fulfill their obligations as part of the Federal response to public health emergencies."

Public Law 107-287, Department of Veterans Affairs Emergency Preparedness Act of 2002 enacted November 7, 2002, requires that the "Secretary take appropriate actions to provide for the readiness of Department medical centers to protect the patients and staff of such centers from chemical or biological attack or otherwise to respond to such an attack so as to enable such centers to fulfill their obligations as part of the Federal response to public health emergencies" and that the "Secretary take appropriate actions to provide for the security of Department medical centers and research facilities, including staff and patients at such centers and facilities." This Act also states that the "Secretary may furnish hospital care and medical services to individuals responding to, involved in, or otherwise affected by that disaster or emergency."

38 USC Sec. 901 gives the Secretary the authority to prescribe regulations to provide for the maintenance of law and order and the protection of persons and property on VA property.

1.2 VA Facilities

The Department of Veterans Affairs (VA) is composed of a Central Office (VACO) and three administrations, the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA). VHA manages one of the largest health care systems in the U.S. In addition to providing health care, VHA also has missions to provide training for health care professionals; to conduct medical research; to serve as a contingency backup to Department of Defense (DoD) medical services; during national emergencies, to support the National Disaster Medical System (NDMS); and provide hospital and medical services, as appropriate, to civilians during community-wide disasters. VBA provides benefits and services to Veterans including compensation and pension, education, loan guaranty, and insurance. NCA delivers burial benefits to Veterans and eligible dependents. In total, VA provides a mission critical medical and economic infrastructure to the government and population of the United States.

Mission critical facilities shall include all VA medical centers and long-term care facilities; major outpatient clinics or clinics in locations where these are the only available health care facilities for a locality; research facilities; major data processing centers; and other facilities which serve a unique function for the Department. Mission critical requirements shall extend to all permanent operational support structures at the facility or medical center. The status of each facility shall be determined by VACO prior to the programming phase of any project.

The facilities in the following list remain as published in the previous version of the Physical Security Design Manual dated July, 2007. VHA is currently planning to conduct a comprehensive review and analysis for the facilities and their physical security designations (i.e. mission critical or life-safety protected). Upon completion of the VHA review and analysis, the updated information will be incorporated into this Manual.

Mission Critical Facility Types

Acute care	Information technology
Ambulatory care	Medical equipment storage
Animal facility	Medical gas storage
Boiler plant	Medical records
Communications center	Medical research
Consolidated mail-out pharmacy	Mental health (inpatient)
Dietetics	National Continuity of Operations Center
Domiciliary	Outpatient clinic
Drug/Alcohol rehabilitation	Psychiatric care facility
Emergency Command Center	Rehabilitation medicine
Emergency generator	Rehabilitation/Prosthetics
Fire/Police station	Security and law enforcement
Hazardous material storage	Water tower, utility supply storage structure
Hospital	

1.2.1 VA Owned Facilities

Mission critical facilities that are owned and operated by VA shall follow the requirements of this document.

1.2.2 VA Medical-Related Leased Facilities

This section provides guidance in the determination of applicable physical security standards for VA medically-related leased facilities. Refer to section 1.10.1 Exceptions, as necessary.

1.2.2.1 Leased built-to-suit facilities up to 150,000 net usable square feet shall follow the requirements in the VA Physical Security Design Manual (PSDM) for Life-Safety Protected Facilities.

1.2.2.2 Leased built-to-suit facilities greater than 150,000 net usable square feet shall have a determination made by the local VAMC Director, with concurrence by the Network Director, and approved by the Under Secretary for Health for Operations and Management or delegated approving official serving as the *authority having jurisdiction* (AHJ) as to whether the facility will be classified as mission critical or life-safety protected. This determination shall be identified and submitted in the original OMB-300 as part of the initial Capital Planning Process.

- When the facility is classified as mission critical, follow VA PSDM for Mission Critical Facilities, as allowable per local, city, and state building codes.
- When the facility is classified as life-safety protected, follow the VA PSDM for Life-Safety Protected Facilities.

1.2.3 Existing – VA Medical-Related Leased Facilities

1.2.3.1 Existing leased facilities up to 150,000 net usable square feet shall comply with The Risk Management Process: An Interagency Security Committee (ISC) Standard dated August, 2013.

1.2.3.2 Existing leased facilities greater than 150,000 net usable square feet shall have a determination made by the local VAMC Director, with concurrence by the Network Director, and approved by the Under Secretary for Health for Operations and Management or delegated approving official serving as the AHJ as to whether the facility will be classified as mission critical or life-safety protected. This determination will be identified and submitted in the future OMB-300 as part of the Capital Planning Process.

- When the facility is classified as mission critical, follow VA PSDM for Mission Critical Facilities, as allowable per local, city, and state building codes. When the facility is classified as life-safety protected, follow The Risk Management Process: An Interagency Security Committee (ISC) Standard dated August, 2013.

1.3 Introduction to Physical Security Concepts

The Physical Security Design Manual for VA Facilities: Mission Critical dated July 2007 is superseded by this physical security design manual. The VA *CD-54 Natural Disaster Non-Structural Resistive Design* (September 2002) is subsumed and superseded by this physical security design manual. The physical protection strategies used to develop this manual are documented in the *Physical Security Strategies Report* (January 10, 2006).

The Physical Security Design Manuals will be updated by interim amendments and revised every three to five years. All PSDM documents are posted and kept current on the CFM Technical Information Library (TIL) website at <http://www.cfm.va.gov/TIL/>.

VA is not adopting the 2010 Interagency Security Committee (ISC) requirements. The *ISC Security Design Criteria* is a controlled document and cannot be distributed to VA A/E consultants.

1.3.1 Concentric Levels of Control and Protection

The physical security of facilities requires the use of concentric levels of control and protection to provide progressively enhanced levels of security to deter, prevent, detect, delay, and respond to *threats* in the protection of assets. The concept of concentric levels of control is to protect the central asset behind layers of security measures such that it is least exposed to the threats. Where a single line of defense might be easily breached, the concentric levels approach offers redundancy in lines of defense that is less likely to be breached.

1.3.1.1 The first point of control, or the outermost level, should be at the perimeter of the property consisting of fences and other barriers with one or two points of entry through gates controlled by police or other guard personnel. In certain urban sites, the building perimeter may be on the property line. Increased levels of screening of persons and vehicles, as the Department of Homeland Security (DHS) threat levels are changed, must be accommodated at the perimeter without burdening surrounding roads with vehicles waiting to enter the site.

1.3.1.2 The second point of control should be at the building perimeter consisting of doors and other openings protected as appropriate to the level of protection needed with or without the first point of control. This includes access control hardware, intrusion detection, surveillance, and, at selected entrances at various times, personnel for control and screening.

1.3.1.3 The third point of control should be to segregate with barriers and hardware generally accessible public and patient areas from staff-only areas such as pharmacy preparation, food preparation, sterile corridors, research laboratories, and building operations and maintenance areas.

1.3.1.4 The fourth point of control should be to segregate authorized from unauthorized staff areas with barriers and access controls such as card reader-activated hardware. Unauthorized areas may include patient records, laboratories, vivariums, and cash-handling tellers.

1.3.1.5 The fifth point of control, at the innermost level, should be to restrict access to *restricted areas* to a minimum with card-reader access controls, *video assessment and surveillance system (VASS)* monitors, intrusion detection alarms, and forced-entry and/or ballistic-resistant construction. Restricted access areas may include security control centers, *select agent* storage, narcotics storage and pharmaceutical caches, and laboratories.

The more effective the *perimeter barrier* and screening are the less protection is needed within the site, such as between buildings, from patient and visitor parking and the building lobby, and from the site entrance to the other buildings on the site. In highly *urban areas* where the VA building may front on a city street with no *standoff* or separation, the building and its occupants can only be protected from hazards of breaking and entering, vandalism, and even explosive or armed attack by *hardening* the building itself to resist, which may lead to undesirable solutions such as façades with minimum openings and a fortress-like appearance.

1.3.2 Crime Prevention Through Environmental Design

VA follows the principles of *Crime Prevention Through Environmental Design* (CPTED, see www.cpted.net). CPTED strategies include elements of natural surveillance, natural access control, and natural territorial reinforcement. CPTED promotes the principles that proper design and effective use of the built environment can discourage, reduce, or remove potential crime risks. CPTED should be used to evaluate VA site and building designs to create and enhance the concentric circles or layers of security protection.

1.3.3 Facilities in Floodplains

Throughout this manual where it is mandatory that construction or equipment be in an area that is not subject to flooding refer to the FEMA flood map information available at <http://www.fema.gov/business/nfip/fmapinfo.shtm>. No new facility shall be constructed in the 100-year floodplain.

1.3.4 Security Operation Requirements

Design decisions for the physical security of a mission critical facility should be based on the concentric levels of control and protection—both physical and operational—as described in section 1.3.1.

1.4 Objectives of VA Physical Security Design

The primary objective of this manual is to provide the design team with the criteria and standards for the full range of strategies available for existing and new buildings to provide unobtrusive protection for VA facilities while safeguarding the Veterans, staff, visitors, and continued operation of the mission critical facilities during a national emergency or a natural or manmade extreme event.

The physical security standards account for VA operations and policies and must be cost effective when implemented. An objective of this manual is to provide cost effective design criteria that will, when constructed and implemented, provide the appropriate level of physical security to VA's mission critical facilities.

1.5 Requirements for Physical Security Subject Matter Specialists

In order to meet the physical security standards of this manual the design team must include a certified physical security specialist as well as a licensed professional structural engineer who has specialized training in blast design and analysis. These specialists shall become part of the design team during the concept phase of any project. This manual assumes the use of qualified physical security and blast experts.

1.5.1 Physical Security Specialist Requirements

The security specialist shall have a minimum of five years' experience in physical security design and shall maintain current certification as Certified Protection Professional (CPP) or Physical Security Professional (PSP) from the American Society for Industrial Security (ASIS). The security specialist must have demonstrated knowledge and experience applying security strategies, such as the application of CPTED, ballistic and forced entry requirements, and electronic security system design as defined in Chapter 10. The résumé of the specialist must be submitted to the VA Project Manager (PM) for review and approval prior to the concept phase of the project. The qualifications of the firm for whom the specialist works must also be submitted with the résumé.

1.5.2 Blast Specialist Requirements

At a minimum, the structural blast specialist shall have a bachelor's degree in structural engineering or a related field and have formal training in structural dynamics and demonstrated experience with the accepted design practices for blast resistant design. The specialist shall have a minimum of five years' experience in performing dynamic analysis in blast resistant design. The résumé of the specialist must be submitted to the VA PM for review and approval prior to the concept phase of the project. The résumé must include a minimum of three projects during the previous two years with similar scope to the project being designed. The qualifications of the firm for whom the specialist works must also be submitted to the VA PM.

1.6 Budgeting and Programming for Physical Security

When establishing a design and a budget for a mission critical project, the key point is that physical security is fully integrated into the program, rather than an added requirement. When physical security is seen as an add-on to an otherwise complete project, the costs for implementation will be higher and the results less satisfactory. As such, it is essential to establish the physical security goals within the capital investment project application phase of the project and to ensure that the budget is set to reflect the physical security requirements within the program goals.

1.7 Risk Assessment of VA Facilities

Risk assessments of existing VA facilities showed that the primary threats faced by the Department continue to be routine criminal activity and violence in the workplace; however, the proximity of some VA facilities to high *vulnerability* targets and the role of VA medical centers as backup to DoD and communities in the public health system elevate VA's risks from both internal and external manmade threats.

It is not possible to eliminate all risk to a facility and every project will face resource limitations. Cost effective risk management is a requirement of every project. As part of the planning phase of a new mission critical facility or major alterations of an existing mission critical facility a risk assessment must be performed, to determine project- or site-specific requirements or modifications to the physical security design requirements, taking into account the *Hazard Vulnerability Assessment (HVA)* and *Comprehensive Emergency Management Plan (CEMP)* for the facility. Cost effective strategies must be implemented to make the facility capable of mission critical operation.

The first task is to identify the assets and people that need to be protected. Next, a threat assessment is performed to identify and define the threats and hazards that could cause harm to a building and its occupants. Threats and hazards shall be measured against the overall facility and each mission critical function and system it contains or supports. After threats and assets are identified, a *vulnerability* assessment is performed to identify weaknesses. Next, the *consequences* to the mission that would result from a hazard event or a successfully executed

threat are defined. Using the results of the asset, threat, vulnerability, and consequences assessment, risk can be determined.

Comprehensive protection against the full range of possible natural hazards and manmade threats to VA facilities would be cost prohibitive, but an appropriate level of protection obtained through the use of these standards can provide for continued operation of mission critical facilities at a reasonable cost.

1.8 Document Distribution, Use, and Control

This manual is unclassified.

1.9 Administration and Enforcement

The provisions of these standards shall apply to all VA mission critical construction projects for which design is begun on or after the effective date of this design manual.

These standards apply to new construction, whether free standing structures, additions, or major alterations. Application of these standards does not extend to other spaces within the existing building, except where directed by VA. Existing facilities not undergoing renovation may be required to meet certain physical security standards defined in this design manual as determined by VA, based on funding considerations, prioritization, and other mission driven requirements.

At any campus where a new mission critical facility is to be constructed, the entire site shall be upgraded to conform to these standards, except when limitation of the project scope or insufficient funding makes it infeasible to do so. Where the entire site cannot be upgraded, the project shall be designed to incorporate achievable physical security elements in a manner that will allow enhancement of those elements in the future. The specific elements to be incorporated or omitted shall be determined, using the risk assessment of both the site and facility, by the VA PM with the concurrence of the VA AHJ for overseeing implementation of physical security requirements for the facility.

Newly constructed roadways and alterations to existing roadways, building access, site access, and site circulation shall be designed in compliance with these standards.

1.10 Interpretations and Exceptions

VA facilities that are not designated mission critical are life-safety protected. Life-safety protected buildings are required to protect the life safety of the patients, staff, and visitors in case of an emergency. Although indispensable to the mission of VA, life-safety protected buildings are not required to remain operational in a natural or manmade extreme event or a national emergency. Physical security design requirements for life-safety protected facilities are covered in a separate manual.

Connecting corridor concourse and bridges, that are not the main entrance or required exit for the connected buildings, shall be exempt from the standoff distance requirements of Chapter 3 and the requirements of Chapters 6 and 7. Freestanding greenhouses shall be exempt from the requirements of Chapters 3, 6, and 7. Physical security requirements for temporary buildings shall be determined on a case-by-case basis by the AHJ for overseeing implementation of physical security requirements for the facility.

1.10.1 Exceptions

When a determination is made at the local level, that due to mission, function, location, or regional responsibility a facility should be upgraded from life-safety protected to mission critical (or vice versa), or when a waiver/deviation from the physical security requirements is sought, a request must be submitted and approved by the AHJ who is responsible for overseeing implementation of physical security requirements for facilities within his or her jurisdiction before the beginning of design.

1.10.2 Procedures for Waivers and Exceptions

The local facility may initiate the waiver and exceptions process. The request shall be submitted to the AHJ for review and approval. For VHA, the AHJ is the Deputy Under Secretary for Operations and Management (DUSHOM) within 10N, and requests shall be submitted through the Network channels to 10N for review. For NCA, the AHJ is the Under Secretary for Memorial Affairs. For VBA, the AHJ is the Office of Administration, Emergency, Preparedness, and Facilities.

1.10.2.1 Waiver or exception requests shall include a narrative with justification for the request. To the extent applicable, include the following information:

- Building category
- Design criteria to be waived
- Physical limitations on implementation imposed by existing conditions
- Programmatic limitations imposed by implementation of standards
- Alternative method of achieving equivalent level of protection or a schedule for phased implementation of standard as part of risk mitigation strategy (VHA only)
- Cost of implementation of design standard with a comparison cost of the proposed equivalent protection
- Funding sources
- Impact of waiver on design schedule, construction schedule, and future operations
- Detailed effects on HVA and CEMP (VHA only)

1.10.2.2 Review and approval procedures for waiver or exceptions shall be as follows:

- Obtain concurrence from the AHJ for overseeing implementation of physical security requirements for the facility
- Forward a copy of the approved waiver/deviation request to the Office of Facilities Planning within the Office of Construction & Facilities Management in VA.

1.11 Master Planning

As part of the master plan development, VA will conduct risk and vulnerability assessments for the facility or campus being planned. The findings of these assessments shall be incorporated into the master plan.

For facilities that have master plans, these plans shall include physical security design guidelines and parameters consistent with those included in, or referenced by, this document. At a minimum, master plans shall include standoff distances, provisions for perimeter security, site access control, applicable CPTED principles, site utility entrances and distribution, a mass evacuation plan, and a schedule for implementation of design guidelines and parameters or approved risk mitigation alternatives.

2 GLOSSARY & ACRONYMS

The following terms and definitions are related to the mitigation of manmade and natural hazards and do not include terms related to general facility design, construction, and operation.

A/E: Architect(s) and Engineer(s) consultants

Alterations: Major alterations or renovations define a project where the area of renovation, including any associated addition, is equal to or greater than 50 percent of the area in the building in which the work is to be performed. In cases where renovations involve changes to the building systems, site work, or other work that does not involve the building interior, the local facility, with concurrence by the region/network and approved by the AHJ shall determine if the work qualifies as a Major Renovation.

Anti-ram: Tested for resistance to a moving load impact at a given velocity and rated in terms of kinetic energy or “K” rating in tests for certification under Department of State programs or “M” rating in tests for certification under ASTM F2656.

Authority Having Jurisdiction (AHJ): The physical security decision-maker for the facility, such as the administration head, assistant secretary, other key official, or deputy assistant secretary, who is responsible for overseeing implementation of physical security requirements for facilities within his or her jurisdiction.

Balanced Design: Controlled failure of a system with an established hierarchy of component failures, where connections are designed for the maximum strength of the connecting components and members supporting other members are designed for the maximum strength of the supported members. For window systems, the glazing shall fail before all other components. (*ASCE/SEI 59-11 Blast Protection of Buildings*)

Cache: A storage facility requiring a high level of security, often referring to facilities storing pharmaceuticals or other supplies for use in emergencies.

Charge Weight: The amount of explosives in a device in trinitrotoluene (TNT) equivalent.

Closed Circuit Television (CCTV): A video system in which an analog or digital signal travels from a camera to video monitoring stations at a designated location. Historically, the term for a security video system was closed circuit television (CCTV), a closed analog video system. Very few video systems today are either closed or completely analog, making CCTV an antiquated term and leading the security industry to use various terms to describe a video system. Because security video serves two distinct purposes, assessment and surveillance, the term used here is video assessment and surveillance system or VASS. This provides a common term based on the functions the system serves, independent of technology.

Comprehensive Emergency Management Plan (CEMP)

Consequences: Consequences assessment looks at the value of a building's critical assets, those that need to be protected, and the importance of the building's operations, within a wider network of public or private activities. (FEMA 452)

Controlled Access Area or Controlled Area: A room, office, building, or facility area which is clearly demarcated, access to which is monitored, limited, and controlled.

Crime Prevention Through Environmental Design (CPTED): Design philosophy that effective use of the natural environment coupled with proper design of the built environment can lead to a reduction in the fear and incidence of crime.

Critical Assets: People and those physical assets required to sustain or support the facility's ability to operate on an emergency basis.

Critical Infrastructure, Critical Space: Building area(s) required to sustain or support the facility's ability to operate on an emergency basis.

Demarc: The separation point between utility-owned and VA-owned equipment.

Department of Agriculture (USDA)

Department of Defense (DoD)

Department of Health and Human Services (HHS)

Department of Homeland Security (DHS)

Detection and Screening System (DSS): DSS are used for the pre-screening of persons, packages, and personal items for detection of contraband, such as, weapons, drugs, explosives, and other potential threatening items or materials prior to authorizing entry or delivery into the building. DSS includes X-ray machines, walk-through metal detectors (WTMD), hand-held metal detectors (HHMD), and desktop and hand-held trace/particle detectors (also referred to a "sniffers" and "itemizers").

Duress Security Phone Intercom (DSPI): DSPI systems are used to provide security intercommunications for access control, emergency assistance, and identification of personnel under duress requesting a security response.

Earthquake Zones: See seismic zones.

Electronic Security System (ESS): A sub-element of the physical security system, an electronic security system is comprised of *Physical Access Control System (PACS)*; *Intrusion Detection System (IDS)*; *Video Assessment and Surveillance System (VASS)*; *Duress, Security*

Phones, and Intercom System (DSPI); and Detection and Screening System (DSS). The ESS is commonly integrated to support correlation of security activity between subsystems.

Essential Electrical System (EES): A system comprised of alternate sources of power and all connected distribution systems, fuel systems, and ancillary equipment designed to ensure continuity of electrical power to designated areas and functions of a health care facility during disruption of normal power sources, and also to minimize disruption within the internal wiring system.

Extraordinary Event or Incident: Events or conditions that exceed locally accepted design practice.

Federal Emergency Management Agency (FEMA)

Fire Command Center (FCC)

General Services Administration (GSA)

Hardening: Reinforcement of the building structure, components, and systems against impact of a blast, a ballistic assault, or ramming.

Hazard Vulnerability Assessment (Analysis) (HVA)

High Risk Area: A location where a threat may be introduced.

Hurricane Areas: Hurricane preparedness requirements apply to VA facilities located within 16 kilometers (10 miles) of the Atlantic Ocean or 16 kilometers (10 miles) of the Gulf of Mexico. These requirements also apply to all inland VA facilities in Florida, Hawaii, and Puerto Rico. Similar requirements, for preparedness against tropical cyclones in the Pacific Ocean, apply to VA facilities located in Guam, American Samoa, and the Philippines. See also ASCE 7-10, section 26.2 Definitions, for Hurricane Prone Regions and Wind-Borne Debris Regions.

ID Check: Examination and verification of personal or vehicle identification visually or by other means.

Illumination Engineering Society of North America (IESNA)

Interagency Security Committee (ISC)

Intrusion Detection System (IDS): A system combining mechanical or electronic components to perform the functions of sensing, controlling, and announcing unauthorized entry into areas covered by the system. The IDS is intended to sound alarms or alert response personnel of an actual or attempted intrusion into an area.

Itemizer: A trace particle detection device capable of identifying both explosives and narcotics.

Life-Safety Protected Facilities: VA facilities which are required to protect the life safety of the patients, staff, and visitors in case of an emergency; although indispensable to the mission of VA, are not required to remain operational in a natural or manmade extreme event or a national emergency.

Local Alarm: An alarm that is annunciated in the immediate vicinity of the protected premises.

Magnetometer or Metal Detector: A walk-through portal or hand-held device designed to detect changes in magnetic fields used to identify hidden metal objects.

Mantrap or Sally-port: A double-door booth or chamber that allows a person to enter at one end, undergo an access identification routine inside the booth, and when the routine is satisfied, the lock on the booth door at other end is released. A mantrap is used in high security environments where absolute access control is required.

Mission Critical Facilities: VA facilities that is required to continue operation during a natural or manmade extreme event or a national emergency.

Mitigation: Actions taken to reduce the exposure to and impact of a hazard.

Pedestrian Barrier: A fence, wall, or other structure designed to delay pedestrians from entering the site without using the gates provided for pedestrians where *personnel screening* may be performed. The pedestrian barrier may or may not be coincident with the vehicle barrier.

National Disaster Medical System (NDMS)

National Terrorism Advisory System (NTAS): formerly the Homeland Security Alert System (HSAS).

Perimeter Barrier: A physical barrier used on the outside of a protected area to prevent, deter, or delay unauthorized entry.

Personal Identification Number (PIN)

Personal Identity Verification (PIV)

Personnel Screening: Examining persons and their possessions for contraband such as weapons, explosives, and chemical or biological agents using magnetometer, x-ray, search, or other device.

Physical Access Control System (PACS): A system combining mechanical or electrical components, such as card readers, keypads, biometrics, and electromagnetic locks and strikes, for the purpose of controlling access and monitoring building entrances, sensitive areas, mission critical asset areas, and alarm conditions.

Physical Security: That part of security concerned with physical measures designed to safeguard people, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard against damage and loss.

Police Operations Unit: An area designed to facilitate the functions of the police and security services, which include the protection of patients, visitors, and employees; the protection of property; and the maintenance of law and order on property under the charge and control of the Department.

Protected Area: An area continuously protected by physical security safeguards and access controls.

Protection Level: The degree to which resources are used to defeat a threat.

Restricted Area: A room, office, building, or facility area to which access is strictly and tightly controlled. Admittance to this area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area.

Risk: The potential for a loss of or damage to an asset.

Screened Vehicle: Motor vehicle that has been examined systematically to determine whether or not a security threat that needs to be mitigated is present.

Screening Vestibule: Designated space or area located for access control between the public building entrance and the lobby which shall be of sufficient space and be provided with power, telecommunications, and data connections for installation of access control and screening equipment that may be used should the need arise.

Secured Door Opening (SDO): A door opening that requires security hardware such as electric strike, door contact, card reader, forced entry rating, or similar feature.

Security Control Center (SCC): A location for security personnel to monitor VASS, alarms, and other security systems and devices. This may be in a separate space or, for small facilities, combined with a guard or reception desk at the entrance.

Seismic Zones: See VA H-18-8: VA Earthquake Design Requirements.

Select Agent: Select agents shall be as defined in Title 42, CFR, Part 73, including pathogens and toxins regulated by both HHS and USDA and non-overlap select agents of HHS.

Standby Electrical System: Generators, switchgear, fuel storage, and distribution equipment necessary to provide standby electrical power to the mission critical facility.

Standoff: Horizontal distance from event to target.

Terrorism: An action that is intended to cause death or serious bodily harm to civilians or noncombatants, when the purpose of such an act, by its nature or context, is to intimidate a population or to compel a government or an international organization to do or to abstain from doing any act.

Threat: The National Infrastructure Protection Plan (NIPP) defines threat as any “natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.” http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Underwriters Laboratory (UL)

Uninterruptible Power Supply (UPS): A device to provide battery power via an inverter to critical equipment during loss of utility power, or until the essential electrical system (EES) or standby generators are online.

Urban Area: A geographic area with a population of more than 50,000 or a population density of at least 1,000 people per square mile (386 per square kilometer) and surrounding census blocks that have an overall density of at least 500 people per square mile (193 per square kilometer).

Vehicle Arrest: Means of stopping a vehicle from breaching a defensive zone (perimeter).

Vehicle Barrier: A passive or active physical barrier consisting of natural or manmade features designed to keep a vehicle carrying explosives at the required standoff distance. This may or may not be coincident with a pedestrian barrier.

Vehicle Inspection: Examining vehicles for contraband such as explosives using physical search, K-9 searches, trace element sampling, x-ray, or other means.

Video Assessment and Surveillance System (VASS): Security video serves two distinct purposes, assessment and surveillance. The term video assessment and surveillance system or VASS is used here. This provides a common term based on the functions the system serves, independent of technology. Formerly referred to as Closed Circuit Television (CCTV).

Vulnerability: Susceptibility to physical injury to persons or damage to systems or functions. Vulnerability refers to the expected outcome in terms of damage, casualties, and business disruption if a threat is carried out or a hazard occurs. Vulnerability is measured by assessing

features that would enhance or diminish building performance during a crime, terrorist attack, or a hazard event. (FEMA 452)

X-ray Screening System: A device or system that inspects the contents of a package or container for concealed explosives or contraband.

3 SITE CONSIDERATIONS

3.0 Scope, Purpose, and Goals

This chapter focuses on security design concepts, elements, and site planning strategies that influence the protection of the built and natural environments.

VA follows the principles of Crime Prevention Through Environmental Design (see www.cpted.net) in order to reduce or remove potential crime risks. CPTED principles should be incorporated into the site design to create and enhance the concentric circles or layers of security protection.

For guidance on construction requirements for site security, such as perimeter fences and other barriers, refer to the Uniform Facilities Criteria (UFC) UFC 4-022-02 and UFC 4-022-01 available on the Whole Building Design Guide (WBDG) (see <http://www.wbdg.org>).

3.1 Standoff Distance

No vehicle shall be parked closer than 50 feet (15 m) to any side of a mission critical VA facility or permanent structure that provides operational support, regardless of the building height.

No unscreened vehicle shall be permitted to travel closer than 50 feet (15 m) and no *screened vehicle* shall be permitted to travel within 5 feet (1.5 m) of any mission critical VA facility. These minimum standoff distances are to be provided to the edge of the curb line demarcating the internal roadways and parking within a VA campus. For facilities not located within a campus with internal roadways or parking, the minimum 50 feet (15 m) standoff is to be provided to site perimeter fence.

3.1.1 Existing Facility – Standoff Distance

Requirements for standoff distance at existing facilities shall be the same as in section 3.1.

3.2 Perimeter Fences

Perimeter barriers shall consist of fences, walls, a combination of these, and gates as needed for access. The perimeter barrier shall be contiguous around the entire facility or the campus within which the facility is located. The barrier shall be designed to resist forced or surreptitious entry using hand tools, such as by spreading bars of a fence to provide a passable opening. Fences shall have sufficient lateral support to resist overturning by manual force. The perimeter barrier, or *pedestrian barrier*, does not have to be *anti-ram* rated unless the barrier serves to mitigate a determined risk. Access gates shall be located to direct pedestrians and vehicles in ways that enhance the operational environment of the security force.

3.2.1 Location

The perimeter barrier shall be located as close as possible to (or along) the property line of the site on which the facility is located such that the standoff distance to the barrier is maximized and satisfies the minimum standoff distance requirements.

3.2.2 Height

The perimeter barrier shall have at least 8 feet (2.4 m) between potential horizontal footholds or designed with other anti-climb measures.

3.2.3 Material

Fences shall be metal and of heavy industrial-grade construction with bar spacing at a maximum of 5 inches (127 mm) on center. Chain link fences and gates shall not be used. Walls shall be of reinforced masonry or concrete construction.

3.2.4 Gates

Gates shall be of the same or similar design and materials as the adjacent fences. Location of the gates shall have standoff from public streets to provide the security force with early warning of approaching pedestrians or vehicles. Gates shall be located away from known criminal adjacencies (such as prisons and high crime areas). The site adjacent to the gates shall provide transitional, non-silhouette lighting, and traffic calming features. Gates shall be access card operated from the outside or as prescribed by the AHJ.

3.2.4.1 Pedestrian gates: Pedestrian and bicycle gates shall swing in the outward direction and shall be fully accessible to persons with disabilities in width and operation.

3.2.4.2 Vehicular gates: Vehicular security gates shall be sliding or cantilevered (no tracks) and only wide enough to accommodate one vehicle lane. The vehicular gates shall be capable of being locked, but do not have to be anti-ram rated.

3.2.5 Existing Facility – Perimeter Fences

All sites with mission critical facilities shall have perimeter fences meeting all the requirements of section 3.2.

3.3 Vehicle and Pedestrian Screening

3.3.1 Guard Houses

Pedestrian and vehicle perimeter entrances shall be provided with enclosed guard houses for guard personnel, gate operation, vehicle inspection, and information.

- Guard houses shall be designed to permit the guard to perform duties from within the guard house and shall have a secondary means of egress.
- Guard house design shall be compatible with the facility architecture and the neighborhood.
- Guard houses shall be heated, air conditioned, and lighted to provide an appropriate work environment.

- Guard houses shall be provided with power, telephone, intercom, data, and other equipment as directed by the VA Police.
- Guard houses shall be protected by bollards and designed to be ballistic resistant, with doors, walls, and windows meeting a UL 752 Level 3 standard.

3.3.2 Vehicle Screening Area

Provide adequate space to accommodate vehicle screening without blocking public rights-of-way.

3.3.2.1 Space and utilities: The screening area shall provide adequate space and site utilities to accomplish the following tasks.

- Visual identity check of driver's license.
- Visual inspection of vehicle interior, including luggage compartment, cargo boxes, and trailers.
- Trace element swipes and sensors.

3.3.2.2 Stacking space: Stacking space shall be provided for vehicles awaiting inspection outside site entrance and off public roads.

- At entrances for employee vehicles, the stacking space shall be sufficient to handle the throughput of vehicles at peak inbound levels.
- At public entrances, stacking space shall be sufficient for average visitor vehicle traffic volume and include space to pull a vehicle aside out of the lane of inbound traffic.

3.3.2.3 Separation: In-bound and out-bound vehicles shall have separate lanes and gates at all vehicular entrances.

3.3.2.4 Reject lane: A turn-around lane shall be provided on the exterior of the entrance gate to permit vehicles to be sent away without interfering with traffic.

3.3.2.5 Parking: Parking shall be provided inside the entrance gate for two police vehicles.

3.3.2.6 Public transportation: Where public transportation is allowed on the VA site for employees and visitors, space shall be provided for the vehicle to be inspected.

3.3.3 Existing Facility – Vehicle and Pedestrian Screening

3.3.3.1 Pedestrian barriers and screening: Any site with an existing mission critical facility shall meet the requirements for pedestrian barriers as described in sections 3.2 and 3.3.

3.3.3.2 Vehicle barriers and screening: Any site with an existing mission critical facility shall meet the requirements for *vehicle barriers* as described in sections 3.2 and 3.3.

- Site utility surveys shall be conducted prior to design and installation.
- Foundations for anchoring the barriers shall be coordinated with existing underground features such as utilities, tunnels, or other subsurface conditions.

3.4 Anti-ram Rated Vehicle Barriers

Active or passive vehicle barriers shall be selected on the appropriateness of the architecture of the facility and the specifics of the site and natural environment.

3.4.1 Active Barriers

Types of active barriers shall be anti-ram rated hydraulic or electric wedges, plate, beam or retractable bollards recessed into the pavement for a flush condition when not deployed. Barriers may be permanently installed or portable type.

3.4.1.1 Locations: At access points that permit vehicles within the minimum 50 feet (15 m) standoff zone around the facility. Examples include access to the loading dock, emergency lanes, and maintenance access. When the 50 feet (15 m) standoff zone coincides with the site perimeter fence, the active barriers are to be located at the vehicle entrances into the site.

3.4.1.2 Structure: See Chapter 7, section 7.4 Anti-ram Resistance, for structural requirements of active barriers.

3.4.1.3 Portable Barriers:

- Each identified location for use shall be provided with necessary utilities and configured in such a way that the barriers may be easily put into place when needed.
- Portable barriers shall be stored with lifts and transport devices to permit rapid deployment in a secure location that is readily accessible by authorized personnel.

3.4.2 Stationary (Passive) Barriers

Anti-ram rated natural or manmade stationary barriers may be used. Landscaping examples include berms, gullies, boulders, trees, and other terrain. Hardscaping examples include benches and planters. Structural examples include walls, bollards, and cables.

3.4.2.1 Locations: Adjacent to *high risk* perimeter fences, protection for site utility equipment, at building entrances, at vehicle or ambulance drop-offs, at cafeterias, gathering areas, and other areas requiring additional protection from vehicles. High risk perimeter fences are portions of the fence at which there is a perpendicular vehicular roadway length equal to or greater than 200 feet (61 m), on which a vehicle can achieve a high approach speed.

3.4.2.2 Structure: See Chapter 7, section 7.4 Anti-ram Resistance, for structural requirements of passive barriers.

3.4.2.3 Accessibility for persons with disabilities: Coordinate locations of passive barriers, such as bollards, with accessibility requirements when placed adjacent to or across a path of pedestrian travel.

3.4.3 Existing Facility – Anti-ram Rated Vehicle Barriers

All sites with mission critical facilities shall meet the requirements for vehicle barriers installed in accordance with section 3.4.

3.5 Parking

3.5.1 Location

No new facilities shall be built with parking in or under the facility.

3.5.1.1 Surface parking: Vehicles shall not be parked or permitted to travel closer than 50 feet (15 m) to any mission critical VA facility.

3.5.1.2 Parking structures: No parking structure, whether on- or offsite, and whether above or below grade, shall be constructed closer than 50 feet (15 m) to any VA mission critical facility. No unscreened vehicles shall be permitted to be parked within or under any VA facility.

3.5.2 Access

3.5.2.1 From vehicle entrance: Access roads for all vehicles shall allow for separate driveways to the building entrance, service yard, or parking.

- Separate entrances to the site shall be provided for patients and visitors, employees and staff, emergency, and service and delivery vehicles.
- Access roads from entrances to parking for each vehicle type shall be separated, but may be connected for maintenance and emergency vehicles through gates controlled by access cards.
- Access roads shall be configured to prevent vehicles from attaining speeds in excess of 25 mph (40 kph).
- Straight-line vehicular approaches to a facility shall be avoided.

3.5.2.2 From parking to facility: See Chapter 4 for information on building entrances.

3.5.3 User Type

In addition to the requirements of sections 3.5.1 and 3.5.2, the following are parking and access requirements for physical security according to specific users.

3.5.3.1 Patients and visitors: Parking and access for patients, visitors, and the persons transporting them to and from the VA facility shall be as convenient as possible to the main entrance, subject to the requirements of section 3.5.1.1. Parking

and facility access shall comply with accessibility requirements for persons with disabilities.

- Where vehicles are unscreened, make site provisions to accommodate a shuttle service for persons needing assistance.
- Accessible shuttle stops or shelters in parking areas.
- Shuttle parking at building entrance.

3.5.3.2 Emergency: Emergency entrance shall be provided with a small parking area for emergency patients and space for ambulances as convenient as possible to the emergency entrance, subject to the requirements of section 3.5.1.1. Ambulances shall be permitted to approach the building directly and not be subjected to the stand-off distance requirements of this chapter.

3.5.3.3 Childcare parents and staff: All requirements for maintaining standoff distance between vehicles and the building shall apply. Child drop-off and pick-up shall be visible from the office of the childcare/development center and shall be monitored by VASS. All vehicular areas, onsite and adjacent offsite, including parking and access roads, shall be separated from playground areas by fences designed to prevent children from entering the vehicular areas and vehicles from entering the playground.

3.5.3.4 Vendors: The standoff distance and screening requirements of sections 3.1 and 3.3 apply. Vendors shall use the delivery vehicle entrance and service yard at the loading dock. Parking shall be provided for vendors in the service yard.

3.5.3.5 Employees: Where employees share access with patients and visitors, the entrance to the employee parking shall be controlled by a card-actuated gate. Employee parking areas shall be monitored by VASS. Emergency alert systems, such as blue phones, shall be provided at the discretion of the VA Police.

3.5.4 Existing Facility – Parking

When separation of types of traffic is not feasible, card-controlled access gates and other traffic separation measures shall be used.

Parking in or under an existing VA facility shall be restricted.

Parking in or under a VA mission critical facility shall be eliminated, where possible. Where parking must remain in or under a mission critical building, all vehicles entering the parking must be screened. Where screened parking is permitted, structural hardening of columns, load bearing walls, and slabs in the garage is to be provided per Chapter 7.

3.5.4.1 Surface parking: Passenger vehicles shall not be parked closer than 50 feet (15 m) to any mission critical VA facility. Existing parking within this standoff distance shall be eliminated, where possible. Where surface parking must remain within the 50 feet (15 m) standoff distance, the VA mission critical facility must be hardened to achieve the performance requirements for the corresponding increase in blast loads. See Chapters 6 and 7 for additional information on the façade and structural hardening requirements.

3.5.4.2 Parking structures: Where parking structure, whether on- or offsite, and whether above or below grade, must remain within the 50 feet (15 m) standoff distance, the VA mission critical facility must be hardened to achieve the performance requirements for the corresponding increase in blast loads. See Chapters 6 and 7 for additional information on the façade and structural hardening requirements.

3.6 Site Lighting

3.6.1 General Requirements

Provide minimum maintained illumination levels for pedestrian pathways, bicycle and vehicle routes, parking structures, parking lots, wayfinding, signage, pedestrian entrances, and building services which will provide safety and security for personnel, buildings, and site. Refer to the VA Electrical Design Manual for illumination requirements. Lighting shall provide for safety and security without compromising the quality of the site, the environment (including neighboring properties), or the architectural character of the buildings.

3.6.1.1 Aesthetic: The site lighting shall provide desired illumination and enhancement of trees, landscaping, and buildings without providing dark shadowy areas compromising safety and security.

3.6.1.2 VASS: Site lighting shall provide VASS and other surveillance support with illumination levels and color that assists in proper identification. Lighting shall be coordinated with VASS cameras to enhance surveillance and prevent interference. Avoid blinding VASS cameras in the placement and selection of fixtures and their cutoff angles.

3.6.1.3 Luminance levels: Illumination levels shall be in compliance with the Illumination Engineering Society of North America (IESNA), VA Electrical Design Guide, and local and state governing agencies.

3.6.1.4 Signage and wayfinding: Shall be enhanced by site lighting, including providing improved security by assisting pedestrians and vehicles to locate their destinations expeditiously. Refer to the latest edition of the VA Signage Design Guide.

3.6.1.5 Environmental: Minimize light pollution and spill into neighboring properties by selection of fixtures' cutoff angles to minimize their nuisance visibility from adjacent areas on and off VA property.

3.6.2 Lighting Locations

Comply with all requirements for site lighting as set forth in VA publications. In addition, the following areas require additional attention in lighting design to support security and safety needs.

3.6.2.1 Site entrances: Lighting shall be provided at all site entrances at illumination levels that assist in after dark performance of security duties.

- To assist guards with visual personal identification into vehicles to see the driver's compartment and view *ID*.
- To assist guards with visual screening of box trucks, cargo areas, trunks, and trailers.
- To provide illumination of wayfinding and other signage.

3.6.2.2 Perimeter fence: Lighting sufficient to support perimeter VASS surveillance shall be provided without objectionable spill onto neighboring properties or rights-of-way. Where a perimeter road has been provided for patrols or other functions, the lighting may be combined with roadway lighting.

3.6.2.3 Building entrances and exits: Lighting at building entrances shall support VASS surveillance and ID functions while providing illumination of surfaces and features for safety.

3.6.2.4 Parking areas: All parking areas covered and open shall be lighted in support of VASS and other surveillance without objectionable spill into adjacent areas on or off site.

3.6.2.5 Pathways: Pedestrian and bicycle pathways and walks, including bike racks, gates, and other features shall be illuminated in support of VASS and other surveillance, while providing for safety without objectionable spill onto adjacent areas on and off site.

3.6.2.6 Signage: All signage shall be adequately illuminated to provide safe wayfinding and identification. Wayfinding maps and texts shall be individually illuminated.

3.6.2.7 Enclosures: Liquid oxygen tanks and other enclosures, such as water tanks/towers and refueling stations, shall be illuminated in support of VASS and visual surveillance without spillage into other areas on- or off site.

3.6.2.8 Trash collection areas: Collection areas shall be illuminated in service yards as a part of the yard illumination. Individual trash bins may not require illumination.

3.6.2.9 Loading docks and associated yards: Loading areas shall be fully illuminated for operations and in support of VASS and other surveillance and identification needs.

3.6.3 Existing Facility – Site Lighting

All sites with mission critical facilities shall have site lighting installed in accordance with section 3.6.

4 BUILDING ENTRANCES & EXITS

4.0 Scope, Purpose, and Goals

This section provides requirements for public entrances, entrance lobbies, patient drop-offs, and staff entrances. Reduce the number of public entrances to the minimum number required. Entrance requirements for specific functional areas, such as emergency department, loading dock, and other service entrances for mission critical facilities, are covered in Chapter 5. Specific requirements for security devices and their locations can be found in Appendix A, Security Door Opening Matrix, and Appendix B, Security System Application Matrix.

4.1 Public Entrances and Lobbies

Public access to the facility should be restricted to a single or limited number of entrances.

4.1.1 Entrances

4.1.1.1 Public entrances: All public entrances to mission critical buildings shall have a *screening vestibule* that may be used when VA requires individuals entering the building to pass through access control and screening prior to entering the building lobby.

4.1.1.2 Staff entrances: Staff entrances shall be located independently of main entrance lobbies and be convenient to staff parking. Provide staff entrances with access control, visual monitoring devices, and intrusion detection system.

4.1.2 Screening Vestibules

The screening vestibule shall have sufficient space and be provided with power, telecommunications, and data connections for installation of access control and screening equipment that may be used should the need arise. Configure access from the drop-off to the lobby through the screening vestibule to prevent circumvention of screening process. Arrange path of travel to prevent vehicular access beyond the standoff distance to the building perimeter. Provide sufficient size to accommodate several people with mobility aids.

The screening vestibule may be one of two types: independent of the main building or part of the main building near the entrance doors. The standoff distance for vehicles may be measured to the main building façade whether the entry vestibule is within the building or an independent structure.

4.1.2.1 Screening vestibules as a separate lobby that is independent of the main building. The preference is for the screening vestibule to be located outside of the VA mission critical facility footprint as a stand-alone structure or structurally isolated from the protected building, such that any damage to the vestibule will not impact the integrity of the VA mission critical facility. When the screening vestibule is a stand-alone or independent structure, the standoff requirements of Chapter 3, the façade

requirements of Chapter 6, and the structural requirements of Chapter 7 are not applicable to the vestibule. However, laminated glass is to be used for all of the screening vestibule's exterior glazing.

4.1.2.2 Screening vestibule as a part of the main building lobby near the entrance doors. When the screening vestibule shares an internal wall or slab with the VA mission critical facility, the internal wall or slab is to be designed as an exterior wall or slab per the requirements of Chapter 6 and Chapter 7. The blast hardening requirements of Chapter 6 and Chapter 7 apply to the exterior wall(s) of the main building lobby.

4.1.3 Primary Public Entrances and Lobbies

4.1.3.1 Location: Vehicles may not approach within 50 feet (15 meters) of the entrance.

4.1.3.2 Doors: Entrance doors to the lobby shall be visible to or monitored by the security personnel in the main lobby. Door operation shall be controlled by security personnel.

4.1.3.3 Access within the facility: Access from the lobby to elevators, stairways, and corridors shall be controlled through the use of electronic access control or mechanical locking devices, limiting access to specific floors and areas that house functions requiring restricted access.

- Install card readers or other electronic access control devices at the entrances to restricted areas. Devices shall be located at entrances to suites and individual rooms from public corridors.
- Install elevator call buttons requiring use of key cards or other electronic access control when they are located in restricted areas.

4.1.4 Access for Emergency Responders

When provided, the Fire Command Center (FCC) and secure house key box for emergency responders shall be located near an entrance door at a location approved by the VA PM, security personnel, and emergency responders. The door associated with the FCC shall be monitored by VASS and controlled by security personnel.

4.1.5 Planning, Construction Details, and Materials

4.1.5.1 Structural: Building entrances shall be constructed to fail in a way that minimizes hazard to persons inside. (See Chapter 6, Building Envelope and Chapter 7, Structural System, for additional requirements.)

- Protection of entrances and lobbies from vehicle ramming shall be accomplished outside and in front of the entrance. (See Chapter 3, section 3.4 Vehicle Barriers.)
- Where a covered drop-off area is provided, its supporting structure shall be independent of the main building and protected from intentional and unintentional damage by vehicles. Protect supporting columns with anti-ram rated barriers and from explosive devices with architectural or structural finishes that prevent detonation within 6 inches.

- Drop-off areas are not permitted beneath the VA mission critical facility footprint.

4.1.5.2 Façade: All glazing (both interior and exterior) in the lobby area shall be laminated glass.

4.1.5.3 Doors and hardware: Exterior doors shall be in size, operation, and other characteristics in compliance with applicable regulatory requirements. Where doors are lockable, they shall comply with emergency egress requirements. Refer to Program Guide (PG-18-14) Room Finishes, Door, and Hardware Schedule, and Appendix A, Security Door Opening Matrix, for additional requirements.

- Glass for entrance and egress doors shall be laminated.
- Entrance doors shall be capable of being remotely locked and unlocked from the reception desk in the main lobby, the *security control center (SCC)*, or other designated position.
- Public entrance doors may be manually or power operated and may be swinging doors, horizontal sliding doors (power operated only), or revolving doors.
- Staff entrance doors shall prevent unauthorized access.
- Residential facilities requiring 24-hour access shall be provided with electronic or mechanical locks on exterior doors as well as visual monitoring and voice communication with connection to information desk or security office.
- Staff entrance door hardware shall include either mechanical or electronic locks.
- Means of egress doors that do not also function as entrances shall be provided with delayed action and alarmed emergency egress hardware.

4.1.5.4 Receptacles: Letter boxes and receptacles for trash and smoking paraphernalia shall not be located within 5 feet (1.5 m) of load-bearing elements. Those within 50 feet (15 m) of the building shall be designed to prevent depositing of explosive charges or to contain explosions with a *W0 charge weight* (defined in the Physical Security Design Standards Data Definitions) as directed by the VA PM and coordinated with the structural engineer.

4.1.6 HVAC

Maintain positive pressure in lobbies and entrance areas.

- Refer to Chapter 9, Building Systems, for requirements regarding relationship of air intakes to drop-off areas.

4.1.7 Security

All public entrances require security monitoring. At public entrances create a “hard line” in the screening vestibule between the entrance and the lobby by providing a guard station with capacity to screen patients, visitors, and packages when screening is required.

4.1.7.1 Security guard stations: Guard stations shall be located at building entrances available to the public. Guard stations shall be located where pedestrian traffic can be monitored and controlled by security personnel. Where guard stations are located outside, they shall be protected from weather and capable of being secured when not in use.

- Guard stations that are incorporated into an SCC shall be separated from public areas with UL 752 Level 3 bullet resistant construction.

- Guard stations that are not incorporated into an SCC shall be provided with a desk and capacity to communicate directly with the SCC.
- An intercom shall be provided from the front door to the guard station reception desk and SCC.

4.1.7.2 Screening devices: At all public entrances provide a screening vestibule with all required connections for temporary installation of *metal detectors* and package screening equipment and sufficient space for their installation and operation.

- Locate screening equipment in a manner that will prevent passage into the building or facility without passing through the devices.
- When screening devices are not permanently installed, provide secure storage in close proximity to their installation location.
- Locate screening equipment so as not to restrict emergency egress.
- Screening devices shall accommodate persons with disabilities.

4.1.7.3 Security devices: VASS cameras shall be provided to monitor activities in the vestibules and lobbies and shall be located to provide views of approaching pedestrian and vehicular traffic, drop-off areas, building entrances, and departing pedestrian and vehicular traffic.

4.1.8 Existing Facility – Public Entrances and Lobbies

4.1.8.1 Covered drop-off: Protect columns with anti-ram barriers such as bollards and from explosive devices by installation of architectural or structural finishes that prevent detonation within 6 inches (152 mm).

4.1.8.2 Vestibules: Where space permits, provide an entrance vestibule of sufficient size to accommodate several people with mobility aids. Configure access from the drop-off to the lobby through the screening vestibule to prevent circumvention of screening process. Arrange path of travel to prevent vehicular access beyond the standoff distance to the building perimeter.

4.1.8.3 Glazing: All glazing (both interior and exterior) in the lobby area shall be laminated glass or fitted with attached anti-fragmentation film.

4.1.8.4 Access within the facility: Modify existing elevator call buttons to require electronic access control to register calls when elevators open directly into restricted areas. Alternatively, construct secure vestibules at elevator lobbies on floors with restricted access.

4.1.8.5 Security devices: VASS cameras shall be required and located in accordance with section 4.1.7.3.

4.1.8.6 Receptacles: Locate as per section 4.1.5.4.

4.2 Patient Drop-offs

Patient drop-offs shall be located at primary building entrances or other locations that will provide convenient access to services without hindering the flow of traffic. Patient drop-off areas shall not be located under occupiable portions of the building or near staff-only entrances.

4.2.1 Vehicular Access

Drop-offs and staging areas for vehicles, including public transportation vehicles, shall be separated from the protected building structure by at least 50 feet (15 m).

4.2.2 Parking

Parking shall not be permitted in patient drop-off areas. This should be designated by pavement markings and signage.

4.2.3 Security

Provide VASS cameras for general surveillance of the area.

4.2.4 Existing Facility – Patient Drop-offs

Patient drop-offs for existing facilities shall meet the requirements of 4.2.

4.3 Building Exits and Life Safety Considerations

Means of egress shall not be obstructed by installation of security devices such as guard stations, screening equipment, or other security devices. Delayed egress and alarmed exits shall comply with applicable codes and regulations.

4.3.1 Site Requirements

Provide an unobstructed and adequately lighted path from each means of egress to a safe location outside the building.

- Where the means of egress is accessible to persons with disabilities, provide an accessible route to a safe location outside the building.
- Where means of egress lead to loading docks or other service areas, direct users away from hazardous and pathological waste storage, mailrooms, and other areas that may be the source of injury or contamination.
- Plan and locate egress paths so that they are not obstructed by the anti-ram barriers or other similar devices.

4.3.2 Planning, Construction Details, and Materials

Construction of building entrances and exits shall be consistent with the requirements for adjacent building envelope elements.

- See Chapter 6 for blast requirements for the building envelope.
- Means of egress doors shall be of construction that makes unauthorized entry from the exterior difficult. Provide hardware that minimizes the opportunity for unauthorized entry by using components such as continuous hinges and astragals.

4.3.3 Security Monitoring

Where means of egress do not also function as access points for the building, provide card reader for authorized users and delayed action, alarmed egress hardware to indicate unauthorized use.

- Provide VASS cameras at locations with alarmed exits, at loading docks, and other areas subject to pilferage.
- Install door status monitors at doors intended to be used only for emergency egress.

4.3.4 Existing Facility – Building Exits and Life Safety Considerations

Existing facilities shall meet the requirements of section 4.3.

5 FUNCTIONAL AREAS

5.0 Scope, Purpose, and Goals

This section discusses the specific spatial functional areas, their relationships, and adjacencies based on physical security requirements. These functional areas require enhanced protection when included in a mission-critical or life-safety protected buildings. The requirements in this section are in addition to requirements stated elsewhere in this document.

Major renovations of existing functional areas within existing facilities shall bring the functional area into compliance with the requirements of this section. Functional areas not undergoing major renovation shall be brought into compliance with the requirements of this section for existing facilities. Additional requirements are shown in Appendix A, Security Door Opening Matrix, and Appendix B, Security System Application Matrix.

This section supplements other related VA standards for construction, space and facility planning criteria, design guides, design manuals, specifications, and details, which remain in full force and effect. Specifically, all requirements of the VA Fire Protection Design Manual (which covers all VA construction) and the OIT Design Guide (which covers all spaces under OIT's purview) remain in effect.

5.1 Agent Cashier

In addition to the requirements of this section: Program Guide (PG-18-9) Space Planning Criteria for VA Facilities, #234 Fiscal Service, shall remain in full force and effect; the requirements of VA Handbook 0730 Security and Law Enforcement, Appendix B, as they apply to fiscal services shall also apply; and VA Program Guide (PG-18-3) Design and Construction Procedures apply.

5.1.1 Adjacencies

The agent cashier shall be located with the transaction window facing a corridor accessible to public and employees, but not opening to a lobby. There shall be no openings to the exterior of the building.

5.1.2 Entrances

The agent cashier space shall be accessed by a door to a corridor which is accessible only to employees of the facility.

5.1.3 Construction

The agent cashier space shall be fully enclosed in 1-hour fire resistive construction extending from structural slab to structure above.

5.1.3.1 Partitions and openings: Partitions and teller windows facing the public corridor shall be UL 752 Level 3 ballistic construction and 15-minute forced entry

construction, including partitions, doors, glazed openings, teller windows, and transaction trays.

- All surrounding partitions and walls, floor, and ceiling shall be permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction, to include above the false ceiling and below a raised floor, shall be done in such a manner as to provide visual evidence of unauthorized penetration.
- Partitions and walls shall be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal shall be spot welded every 6 inches (150 mm) to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.
- Pass through devices shall meet the same requirement for ballistics and forced entry protection.

5.1.3.2 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through an agent cashier space shall be protected with either bars or grills. Where one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²), bars are not required; however, all ducts shall be treated to provide sufficient sound attenuation. Where bars are used, they shall be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six inches (150 mm) on center; where grills are used, they shall be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.

5.1.4 Security

5.1.4.1 VASS: The agent cashier space and the transaction window shall be monitored by VASS, and as required by the program.

5.1.4.2 Duress alarm: A duress alarm shall be provided in a location not visible to customers at the transaction window.

5.1.4.3 Door: Entrance door shall be controlled and monitored.

5.1.5 Existing Facility – Agent Cashier

Existing agent cashier areas shall provide the security requirements of section 5.1.

5.2 Caches

In addition to the requirements of this section: Program Guide (PG-18-9) Space Planning Criteria for VA Facilities, #268 Pharmacy Service, shall remain in full force and effect; the requirements of VA Handbook 0730 Security and Law Enforcement, Appendix B, as they apply to pharmacy drug storage shall also apply to *caches*; and VA Program Guide (PG-18-3) Design and Construction Procedures apply.

5.2.1 Adjacencies

Caches located within the main facility shall be on a corridor leading to the loading dock, but no closer than 50 feet (15 m) to the loading dock or mailroom. Caches may be located in a separate building from the main facility on the VA facility site, subject to these requirements.

5.2.2 Entrances

Doors and frames to caches shall be opaque hollow metal, and shall be controlled and monitored as follows.

- From exterior to cache with no door from cache to interior of main building.
- From an interior corridor to the cache.

5.2.3 Construction

Caches shall be enclosed in fire rated construction with surrounding construction 15-minute forced-entry resistant. Exterior construction shall be reinforced masonry or equivalent.

5.2.3.1 Partitions and openings: Interior partitions shall comply with the following when separating a cache from other building spaces, including corridors.

- Walls, floor and ceiling shall be permanently constructed and attached to each other. All construction, to include above the false ceiling and below a raised floor, shall be done in such a manner as to provide visual evidence of unauthorized penetration.
- Walls shall be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal shall be spot welded every 6 inches (150 mm) to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.
- No windows, hatches, access panels, or skylights shall be permitted in caches.

5.2.3.2 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through a perimeter partition of the cache shall be protected with either bars or grills. Where one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²), bars are not required; however, all ducts shall be treated to provide sufficient sound attenuation. Where bars are used, they shall be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six inches (150 mm) on center; where grills are used, they shall be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.

5.2.3.3 Electrical: All lighting, security devices, and refrigerators within the cache shall be backed by the standby electrical system. Refer to the VA Electrical Design Manual for specific loads to be connected to the EES.

5.2.4 Security

Entrance doors to the cache and vault doors, if any, within the cache shall be monitored by VASS, controlled by physical access control, and monitored by intrusion detection system (both boundary and volumetric).

5.2.5 Existing Facility – Cache

Existing caches shall comply with the requirements of section 5.2.

5.3 Childcare/Development Center

This section supplements Program Guide (PG-18-9) Space Planning Criteria for VA Facilities, #420 Childcare/Development Center which shall remain in full force and effect.

Childcare/development centers shall also meet the licensure requirements of the jurisdiction in which they are located, as well as the requirements of VA Handbook 0730 Security and Law Enforcement, Appendix B, as they apply.

5.3.1 Adjacencies

When located within a portion of a main VA facility, such as a hospital, childcare/development centers shall be located on the ground floor away from main building entrance with separate access area for drop-off and pick-up.

5.3.2 Entrances

Doors shall be provided with an intercom to the reception desk with remote access from the desk.

5.3.2.1 Public entrances: Doors to childcare/development centers, including the main entrance and secondary entrances, shall be controlled and monitored.

5.3.2.2 Emergency exits: Emergency egress doors from childcare/development centers shall be controlled and monitored.

5.3.3 Construction

No additional physical security requirements.

5.3.4 Security

All entrances, including drop-off and pick-up areas, playgrounds, and other outdoor areas where children may be while at the childcare/development center shall be monitored by VASS.

5.3.5 Existing Facility – Childcare/Development Center

Entrances and security for existing childcare/development centers shall comply with the requirements of sections 5.3.2 and 5.3.4.

5.4 Main Computer Room

This section applies to the main computer room. In addition to the requirements of this section, NFPA 75: Protection of Electronic Computer/Data Processing Equipment shall apply. This section supplements the Office of Information and Technology Design Guide.

5.4.1 Adjacencies

The main computer room shall not be located in a *high risk area* and shall be located not closer than 50 feet (15 m) in any direction to main entrance lobbies, loading docks, and mailrooms, critical utilities, and in no case directly above or below such spaces.

5.4.2 Entrances

Entrance doors to the main computer room and other computer rooms shall be controlled and monitored.

5.4.3 Construction

Surrounding walls and partitions shall be fire resistive construction and extend from slab to slab.

5.4.3.1 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through a perimeter partition of the main computer room shall be protected with either bars or grills. Where one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²), bars are not required; however, all ducts shall be treated to provide sufficient sound attenuation. Where bars are used, they shall be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six inches (150 mm) on center; where grills are used, they shall be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.

5.4.3.2 Power: The main computer room equipment and its supporting HVAC services shall be backed by the standby electrical system. Refer to the VA Electrical Design Manual for specific loads to be connected to the EES and UPS power.

5.4.4 Security

All doors between the computer room and public space shall have motion-activated VASS camera coverage on the computer room side of the door. The space shall be controlled by physical access control and monitored by intrusion detection system (boundary only).

5.4.5 Existing Facility – Main Computer Room

Existing main computer rooms shall comply with the requirements of section 5.4.

5.5 Emergency Department

This section supplements Program Guide (PG-18-9) Space Planning Criteria for VA Facilities, #262 Ambulatory Care (Hospital Based).

5.5.1 Adjacencies

5.5.1.1 Vehicular Access: Only ambulances and emergency vehicles shall be allowed within 50 feet (15 m) of the emergency department entrance; however, no vehicle

shall be allowed within 5 feet (1.5 m) of the building structure. No other vehicles or traffic shall be allowed within 50 feet (15 m) of the emergency department entrance.

5.5.1.2 Functional adjacencies: Provide direct observation of the waiting room from the guard station and direct access through a door controlled and monitored.

- Locate adjacent to *police operations* room or as close thereto as feasible.
- Locate at least 50 feet (15 m) from loading docks, mailrooms, and public lobbies.
- Maximize separation from high risk areas.

5.5.2 Entrances

Provide separate entrances for ambulatory patients and patients arriving by ambulance.

Provide space for screening of pedestrians (see 5.5.4 Security).

5.5.2.1 Exterior doors: Entrances from the exterior shall be controlled and monitored.

5.5.2.2 Interior entry doors: Doors separating the emergency (urgent care) area to the main building shall be solid core wood or hollow metal and controlled and monitored on both sides; doors may have vision panels.

5.5.3 Construction

5.5.3.1 Anti-ram barriers: Refer to Chapter 3 and Chapter 7.

5.5.3.2 Façade: Refer to Chapter 6.

5.5.3.3 Construction separation: Separate treatment area and nurses' station from waiting area and entrances with full height construction. Glazing in this separation shall be laminated glass.

5.5.3.4 HVAC

- Locate all outdoor air intakes at least 50 feet (15 m) from ambulance parking areas.
- HVAC system serving the emergency department shall be independent of systems serving other parts of the facility.

5.5.4 Security

Provide a guard station and direct connection to the SCC, with capacity to screen patients, visitors, and packages at the ambulatory patient entrance.

5.5.4.1 Exterior: Provide VASS cameras capable of monitoring activity at the ambulance entrance and ambulance parking area and that display in the primary and secondary SCC.

5.5.4.2 VASS: Provide VASS monitoring of ER Reception/waiting room and entrance from the exterior.

5.5.4.3 Duress alarm: Provide duress alarm for receptionist, in areas such as the nurses' station, triage, and as required by the program.

5.5.5 Existing Facility – Emergency Department

Existing emergency (urgent care) areas in existing buildings shall meet the requirements of sections 5.5.2 and 5.5.4.

Existing Facility – Entrances: Replace existing glass with laminated glass or install anti-fragmentation film on existing glass near the emergency department entrance.

5.6 Emergency and/or Standby Generator Room

See also the requirements in Chapter 8, Utilities and Building Services, and Chapter 9, Building Systems. Refer to Chapter 6, Building Envelope, for blast protection requirements.

5.6.1 Adjacencies

Emergency and/or standby generators and related switchgear may be located in a separate structure from the main building or within the main building.

5.6.1.1 Elevation: The generator room shall not be located below grade or in a high risk area.

5.6.1.2 Location in building: When within a main building such as a medical center, the generator room shall not be located closer than 50 feet (15 m) of lobbies, loading dock/receiving area, mailrooms, or parking and shall not be located above or beneath such facilities.

5.6.1.3 HVAC: In hurricane prone areas, areaways and louver openings serving the generator shall be hurricane resistant (refer to section 6.5) and shall not open to the service yard for the loading dock. Refer to Chapter 9, Building Systems, for additional requirements.

5.6.2 Entrances

5.6.2.1 Exterior doors: Entrances from the exterior shall not open to the loading dock service yard. Doors shall be hollow metal and controlled and monitored.

5.6.2.1 Interior entry doors: Entrances from the interior of the building shall be fire resistive construction and shall be controlled and monitored.

5.6.3 Construction

Emergency and/or standby generators and related switchgear shall be surrounded by fire resistive construction.

5.6.4 Security

Generators operation and status shall be monitored in the SCC as well as at the engineering control center.

5.6.5 Existing Facility – Emergency and/or Standby Generator Room

Where generators are adjacent to loading docks, mailrooms, or other potentially hazardous locations or may be subject to damage due to structural collapse, a blast mitigation analysis shall be performed and mitigation measures of hardening or relocation shall be taken.

- Doors shall be controlled and generators shall be monitored as required by sections 5.6.2 and 5.6.4.
Louvered openings serving the generator shall comply with requirements of section 5.6.1.3.

5.7 Energy Center/Boiler Plant

See also the requirements in Chapter 8, Utilities and Building Services, and Chapter 9, Building Systems.

5.7.1 Adjacencies

The energy center/boiler plant may be located within a main building or in an independent building. When in an independent building, see Chapter 3 for site planning requirements.

5.7.1.1 Elevation: The energy center/boiler plant, including emergency and/or standby generators and switchgear, and engineering control center, and access to fuel tanks, shall be above grade and shall not be located in a high risk area.

5.7.1.2 Location in building: Where within a main building such as a medical center, the energy center/boiler plant shall not be located closer than 50 feet (15 m) of a lobby, loading dock/receiving area, or mailroom and shall not be located above or beneath such facilities.

5.7.1.3 HVAC: In hurricane prone areas, louvers shall be hurricane and debris impact resistant (refer to section 6.5). Areaways and louver openings serving the energy center/boiler plant shall not open to the service yard for the loading dock and mailroom. Refer to Chapter 9 for additional requirements.

5.7.2 Entrances

The energy center/boiler plant shall not be entered from the service yard for the loading dock and/or mailroom.

5.7.2.1 Exterior doors: Doors shall be hollow metal and controlled and monitored.

5.7.2.1 Interior entry doors: Entrances from the interior of the building shall be fire resistive construction and shall be controlled and monitored.

5.7.3 Construction

No additional physical security requirements.

5.7.4 Security

VASS shall be provided to monitor any entrance to the energy center/boiler plant from the exterior.

5.7.5 Existing Facility – Energy Center/Boiler Plant

Access to the energy center/boiler plant shall be controlled and monitored as required by sections 5.7.2 and 5.7.4.

- Louver openings serving the energy center/boiler plant shall comply with requirements of section 5.7.1.3.

5.8 Fire Command Center (FCC)

When the fire command center designated for use by emergency responders is provided, this section is applicable.

5.8.1 Adjacencies

Location of the fire command center shall be determined with the participation of the facility and emergency responders. It shall be easily accessible in case of an emergency and readily identifiable from a distance of at least 50 feet (15 m).

5.8.2 Entrances

Entrance to the fire command center shall remain locked at all times. Only emergency responders shall have access to this room.

5.8.3 Construction

Surrounding construction shall be UL 752 Level 3 forced entry resistant. Enclosure shall be 2-hr fire resistance rated construction.

5.8.4 Security

No additional requirements.

5.8.5 Existing Facility – Fire Command Center

Existing fire command centers shall meet the requirements of section 5.8 except that they need not have a forced entry resistance rating.

5.9 Incident Command Center

5.9.1 Adjacencies

When provided, the incident command center shall be centrally located in an area of the building that is easily accessible from all other parts of the facility and remote from high risk locations. Where possible, it should have access to natural light and a view of surrounding areas. During normal conditions without incidents or other emergencies, the space may serve other functions such as a conference room.

5.9.2 Entrances

Provide electronic access control at each entrance.

5.9.3 Construction

Surrounding construction shall extend from floor slab to underside of slab above.

5.9.3.1 HVAC: Heating, ventilating, and air conditioning systems shall remain operational at all times.

5.9.3.2 Electrical: All circuits in the incident command center shall be backed by the standby electrical system. Refer to the VA Electrical Design Manual for specific loads to be connected to the EES. Communications and data connections shall be provided with redundancy so that they can be rerouted if connections are lost.

5.9.4 Security

Incident command center shall have secure storage facilities for communications devices outfitted so that equipment is fully charged and ready to use when needed.

5.9.5 Existing Facility – Incident Command Center

Existing incident command centers shall meet the requirements of section 5.9.

5.10 Loading Dock and Service Entrances

5.10.1 Adjacencies

Loading docks shall be adjacent to, but structurally separate from, any VA facility.

5.10.1.1 Prohibited adjacencies: Loading docks shall not be located adjacent to or within 50 feet (15 m) of the following.

- Incident command center
- Fire command center
- Security control center and police operations room
- Emergency or standby generators
- Main computer room
- Water storage tanks
- Main electrical switchgear
- Air intakes
- Main utility service entrances
- Emergency egress from main building
- Childcare/development centers
- Flammable liquids or gas storage
- Outdoor air intakes
- Pharmacy
- Central sterile processing and distribution
- Caches
- Emergency rooms
- Patient care areas

5.10.1.2 Coordination with vivarium: Research animals and animal pathological waste shall have separate loading dock facilities, but may be served by the same service yard as the general loading dock.

5.10.2 Entrances

Pedestrian doors, stairs, and ramps associated with loading docks shall be restricted to authorized personnel and be separated from the loading platform by not less than 4 feet (1.2 m) to discourage by-passing the entry door controls through the loading platform and other doors.

Provide electronic locks and door status monitors on doors serving loading docks.

5.10.2.1 Exterior doors: Exterior pedestrian entrance doors and frames shall be constructed of heavy duty hollow metal and shall be controlled and monitored.

5.10.2.2 Interior entry doors: Doors and frames from the mailroom to the interior of the building shall be fire resistive construction and controlled and monitored.

5.10.3 Construction

5.10.3.1 Structural: When located within the main building, structural columns passing through the loading dock and floor slabs above it shall be structurally hardened to sustain an explosion within the loading dock from a charge weight (defined in the Physical Security Design Standards Data Definitions) as directed by the VA PM. Refer to Chapter 6, Building Envelope, and Chapter 7, Structural System, for additional requirements.

5.10.3.2 Interior partitions: The loading dock and receiving area shall be separated from the corridors and spaces adjoining with reinforced masonry walls and doors of hollow metal construction controlled and monitored. See Chapter 7.

5.10.3.3 Secured storage: Provide secure storage areas for delivered items awaiting uncrating and distribution within the facility and for hazardous and pathological wastes.

5.10.3.4 HVAC

- Locate all outdoor air intakes at least 50 feet (15 m) horizontally and 30 feet (9 meters) vertically from parking areas or on roof away from the roof line.
- Air serving the loading dock and receiving areas shall not circulate to other parts of the building.

5.10.4 Security

An area that is of sufficient size to conduct necessary inspections shall be provided within the receiving area for inspection and imaging of goods received.

5.10.4.1 Guard post: When a second guard post is provided for a building, it shall be located where the loading dock and associated doors can be seen and door status and other access control devices monitored by the guard.

- The guard's office may be near the loading dock supervisor or manager.
- Doors to the guard booth shall be controlled and monitored.

5.10.4.2 Exterior: Install VASS cameras to provide surveillance of all loading dock areas, including the gate, vehicle inspection areas, service yard and various containers, parked vehicles, loading and unloading activities, and building entrances at the loading dock

5.10.4.3 VASS: The loading dock, including vehicles parked at the dock, shall be monitored by VASS.

5.10.4.4 Access control: Dock lift controls and overhead door controls shall be secured with a card reader device to prevent unauthorized use for entry.

5.10.5 Additional Requirements

Loading docks shall be served from service yards enclosed by a secure fence or wall and power-operated sliding gate, controlled by card access device and/or remote release and operation by a guard, the dock manager, or other authorized person with intercom and VASS ID.

5.10.5.1 Vehicle access: Vehicle access to the loading dock shall be restricted.

- Approaches to loading docks shall be configured to limit the speed by any type of vehicle to 25 mph (40 kph).
- Where the entrance gate to a service yard is directly from a public right-of-way, deployable anti-ram rated vehicle barriers shall be provided on the inside of the gate, and shall be integrated with gate controls.
- Provide an area for the inspection of delivery vehicles that will not interfere with the flow of traffic on public rights of way, the site, or the loading area.

5.10.5.2 Service yards: The yard shall be segregated from other vehicle and pedestrian traffic areas by screen walls.

- Delivery vehicle maneuvering and parking shall be within an enclosed service yard accessed by delivery vehicle roadways leading directly from the site perimeter.
- Trash, medical/pathological waste, and other containers, compactors, and other similar equipment shall be located within the enclosed service yard and under VASS.

5.10.6 Existing Facility – Loading Dock and Service Entrances

Loading docks in existing facilities may remain in their original locations. Enclosed service yards as described in section 5.10.5.2 shall be provided. Existing loading docks shall meet the requirements of section 5.10.3.2 and the following.

5.10.6.1 Inspection area: An area that is of sufficient size to conduct necessary inspections shall be provided within the receiving area for inspection and imaging of goods received.

5.10.6.2 Structural hardening: See Chapter 7.

5.10.6.3 Adjacencies: Research laboratories and vivariums in existing buildings may be served by existing loading docks; however, loading of animals and removal of animal pathological waste shall be screened from public view and shall be within a controlled access yard or area.

5.11 Mailroom

5.11.1 Adjacencies

Mailrooms may be located in the main building or in a separate structure on the site shared with loading dock, storage, and other non-critical functions. Mailrooms within the main building shall be located on an exterior wall.

5.11.1.1 Location: Mailrooms within the main building shall be located on an exterior wall and adjacent to the loading dock.

5.11.1.2 Prohibited adjacencies: Mailrooms shall not be located adjacent to or within 50 feet (15 m) of the following.

- Incident command center
- Fire command center
- Security control center and police operations room
- Emergency or standby generators
- Main computer room
- Water storage—domestic and fire
- Main electrical switchgear
- Main utility service entrances
- Emergency egress from the main building
- Childcare/development centers
- Flammable liquids or gas storage
- Outdoor air intakes
- Central sterile processing and distribution
- Cache
- Emergency rooms
- Patient care areas

5.11.2 Entrances

Subject to emergency exit safety requirements, lock all outside doors and prohibit doors from being propped open

5.11.2.1 Exterior doors: Exterior entrance doors and frames shall be constructed of heavy duty hollow metal and shall be controlled and monitored.

5.11.2.2 Interior entry doors: Doors and frames from the mailroom to the interior of the building shall be fire resistive construction and controlled and monitored.

5.11.3 Construction

When located within the main building, structural columns passing through the mailroom and inspection area and floor slabs above them shall be structurally hardened to sustain an explosion within the mailroom or inspection area from a charge weight (defined in the Physical Security Design Standards Data Definitions) as directed by the VA PM. Refer to Chapter 6, Building Envelope, and Chapter 7, Structural System, for additional requirements.

5.11.3.1 Mailboxes: Mailboxes, when provided, shall be in a separate room from the mailroom and inspection area, and shall comply with the mounting heights and other

regulations of the US Postal Service. Unscreened incoming mail shall be housed in a room that is separate from and exterior to outgoing mail.

5.11.3.2 Interior partitions: The mailroom shall be separated from the mailbox room, corridors, and spaces adjoining with reinforced masonry walls and doors of hollow metal construction.

5.11.3.3 HVAC:

- The mailroom shall have separate, dedicated air handling units.
- The incoming mail room and package screening areas shall have dedicated exhaust system to maintain negative air pressure with respect to adjacent spaces.
- Areas housing screened mail shall have separate, dedicated air handling units and maintain positive pressure with respect to areas housing unscreened mail.
- The mailroom shall have a dedicated thermostat control unit and cut-off switch to be able to shut off ventilation to the mailroom. Air serving the mailroom shall not circulate to other parts of the building.

5.11.4 Security

An area that is of sufficient size to conduct necessary inspections shall be provided within the receiving area for inspection and imaging of mail received. This may be space shared with the loading dock inspection area.

5.11.4.1 VASS: The mailroom, including the inspection area, and the exterior loading area serving the mailroom shall be monitored by VASS.

5.11.5 Additional Requirements

5.11.5.1 Separate processing area should include appropriate personnel protection equipment and disposal instructions for such equipment, as approved by the CDC.

5.11.6 Existing Facility – Mailroom

Existing mailrooms shall comply with the requirements of section 5.11.

5.12 Pharmacy

In addition to the requirements of this section: Program Guide (PG-18-9) Space Planning Criteria for VA Facilities, #268 Pharmacy Service, *Clinical Series Pharmacy Service VA Design Guide* and the *Primer Series Pharmacy Design Guide*, which shall remain in full force and effect; the requirements of VA Handbook 0730 Security and Law Enforcement, Appendix B, as they apply to pharmacy drug storage apply; and VA Program Guide (PG-18-3) Design and Construction Procedures apply.

5.12.1 Adjacencies

Deliveries to and shipments from pharmacies may be via the main loading dock and service yard. Pharmacies shall not be immediately adjacent the loading dock or mailroom or other high risk areas.

5.12.2 Entrances

The pharmacy shall be accessed by a door to a corridor which is accessible only to employees of the facility.

5.12.3 Construction

5.12.3.1 Exterior walls: Construction shall be reinforced masonry, or equivalent. Exterior walls composed of metal or wood frame shall have an interior backing of steel security screen mesh or sheet partition.

- Windows or skylights below 18 feet (4 m) from ground level or the roof of a lower abutment, or less than 18 feet (4 m) from windows of an adjoining building, or accessible by a building ledge leading to windows of other floor rooms, shall have forced entry construction of stainless steel woven security mesh.

5.12.3.2 Interior construction: Interior partitions between the pharmacy and surrounding spaces shall be 15-minute forced entry construction and extend from slab to slab.

- All surrounding partitions and walls, floor, and ceiling shall be permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction, to include above the false ceiling and below a raised floor, shall be done in such a manner as to provide visual evidence of unauthorized penetration.
- Partitions and walls surrounding the perimeter of the pharmacy shall be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal shall be spot welded every 6 inches (150 mm) to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.
- Windows or skylights below 18 feet (4 m) from ground level or the roof of a lower abutment, or less than 18 feet (4 m) from windows of an adjoining building, or accessible by a building ledge leading to windows of other floor rooms, shall have forced entry construction of stainless steel woven security mesh.

5.12.3.3 Dispensing partitions and openings: Partitions at the dispensing window and dispensing windows facing the public corridor shall be UL Level 3 ballistic construction and 15-minute forced entry construction, including partitions, doors, glazed openings, teller windows, and transaction trays.

5.12.3.4 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through a perimeter partition to the pharmacy shall be protected with either bars or grills. Where one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²), bars are not required; however, all ducts shall be treated to provide sufficient sound attenuation. Where bars are used, they shall be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six inches (150 mm) on center; where grills are used, they shall be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.

- HVAC services shall remain operational 24 hours/day, 7 days/week.

5.12.3.5 Electrical: All lighting, security devices, and power shall be backed by the standby electrical system. Refer to the VA Electrical Design Manual for specific loads to be connected to the EES.

5.12.4 Security

Provide VASS monitoring of pharmacy dispensing area, vault entrance, and controlled substance storage.

5.12.4.1 Intrusion detection: Provide door and lock status sensors and motion detectors in pharmacy. When the pharmacy is in continuous operation, volumetric intrusion detection is not required.

5.12.4.2 Access control: Pharmacy entry and narcotic vaults shall be controlled via card readers. Mechanical cypher locks shall not be used.

5.12.4.3 Duress alarm: Provide duress alarm at patient transaction counter and patient/pharmacist consult areas, and as required by the program.

5.12.4.4 VASS: VASS shall be used at entry points, exit points, service interaction areas and windows, and waiting areas.

5.12.5 Existing Facility – Pharmacy

Existing pharmacies shall comply with the requirements of section 5.12.4.

5.13 Police Operations Room and Holding Room

This section supplements the following documents which shall remain in full force and effect: Program Guide (PG-18-9) Space Planning Criteria for VA Facilities, #279 Police and Security Service and VA Handbook 0730 Security and Law Enforcement that is in effect at the time this manual is published.

5.13.1 Adjacencies

5.13.1.1 Police operations room: Shall be located, in accordance with VA Handbook 0730, on the first floor of the main patient care building adjacent to the highest potential trouble area, such as admissions, emergency or urgent care room, or lobby and shall be located to allow appropriate response and deployment to respond to a security related event.

5.13.1.2 Holding room: Shall be located within or adjacent to the police operations room.

- An additional holding room may be located within or adjacent to a perimeter screening facility.

5.13.2 Entrances

5.13.2.1 Police operations room: Doors shall be from a corridor used only by staff and shall be controlled and operated.

5.13.2.2 Holding room: Doors and frames shall be heavy gauge hollow metal steel construction and door hardware shall be UL 752 Level 3 forced entry rated controlled and monitored.

5.13.3 Construction

5.13.3.1 Police operations room: When the police operations room is adjacent to or opens onto areas occupied by unscreened public, such as lobbies, elevator lobbies, emergency rooms, and public corridors, construction, including partitions from slab to slab, doors, windows, and other openings separating the unit from such spaces, shall be fire resistive, UL 752 Level 3 ballistic-resistant.

5.13.3.2 Holding room: Construction of the holding room shall be UL 752 Level 3 forced entry resistant and as follows.

- Walls shall be constructed of reinforced masonry extended to the underside of the structure above; drywall and steel stud construction shall not be used.
- Door frames shall be grouted solid and anchored into the masonry walls.
- An observation window consisting of reflective glass protected by clear polycarbonate shall be provided.
- The interrogation table shall be firmly anchored to the floor and to one wall.
- Shackle hasps shall be anchored to wall construction and be capable of resisting pullout of not less than 500 pounds (228 kg).
- Provide anti-ligature construction.
- Vandal resistant products shall be used within the space. Any product within the space with screws shall be tamper resistant.
- Construction and materials shall eliminate opportunities for detainee to inflict self-injury and improvise weapons that could be used to harm others.

5.13.3.3 Power: Police operations rooms and holding rooms shall be backed by the standby electrical system. Refer to the VA Electrical Design Manual for specific loads to be connected to the EES.

5.13.4 Security

VASS surveillance of the entire holding room shall be provided through an opening glazed with transparent polycarbonate in a steel frame firmly anchored to the wall. When requested by the VA PM, the VASS camera shall be covert and use lenses made for the purpose.

5.13.5 Existing Facility – Police Operations Room and Holding Room

Existing police operations rooms and holding rooms in existing facilities, when a police operations room opens directly to other parts of the building, including corridors and elevator lobbies, partitions and control doors shall be constructed to separate the lobby as required by sections 5.13.2, 5.13.3, and 5.13.4.

5.14 Records Storage and Archives

In addition to the requirements of this section, Department of Veterans Affairs publication, Essential Records Vulnerability Assessment (October 2003) shall apply.

5.14.1 Adjacencies

Records storage rooms shall be located not nearer than 50 feet (15 m) in any direction from main entrance lobbies, loading docks, mailrooms, and other high risk areas and in no case directly above or below such spaces.

5.14.2 Entrances

Entrances to archival storage spaces, including book stacks, computer main frames, and valuable or historical records and collections shall be controlled and monitored.

- Emergency egress doors from archival storage spaces shall be controlled and monitored and shall have motion-activated VASS camera coverage of the egress side of the door with all device monitors at a central location within the archival or library area.

5.14.3 Construction

Records storage rooms shall comply with National Archives and Records Administration (NARA) Facility Standards for Records Storage Facilities – Part 1228, Subpart K.

- Where electronic media or data storage facilities are essentially computer rooms, the area shall comply with the requirements of section 5.4.

5.14.4 Security

Archives for rare and valuable artifacts and documents shall be provided with intrusion detection and VASS. The intrusion detection system shall provide boundary and volumetric protection. This space shall be controlled via a card reader.

5.14.5 Existing Facility – Records Storage and Archives

Existing records storage facilities shall comply with sections 5.14.2 and 5.14.4.

5.15 Research Laboratory and Vivarium

This section supplements Program Guide (PG-18-9) Space Planning Criteria for VA Facilities, #278 Research and Development, which shall remain in full force and effect. The requirements of VHA Handbooks 1200.8, 1200.6; Memo dated 2007– BSL Research Lab Physical Security Inspections shall remain in effect. The requirements of Laboratory Security and Emergency Response Guidance for Laboratories Working with Select Agents (CDC Biosafety in Microbiological and Biomedical Laboratories (BMBL) 4th Edition, Appendix F) shall apply to facilities storing and handling select agents. (Select agents shall be as defined in Title 42, CFR, Part 73, including pathogens and toxins regulated by both HHS and USDA and non-overlap select agents of HHS.) Veterinary Medical Unit vivarium spaces shall comply with AAALAC accreditation requirements.

5.15.1 Adjacencies

Laboratories and other spaces storing or using select agents may be in an independent building or within a building such as a medical center.

5.15.1.1 Shared occupancy: When located within a building with other occupancies, the laboratory shall be located on a corridor restricted to authorized employee use.

5.15.1.2 Select agents: Laboratories and other facilities using select agents shall be located no closer than 50 feet (15 m) from public lobbies, mailrooms, loading docks, or other high risk areas.

5.15.2 Entrances

Research and vivarium entrances shall be located away from public areas.

5.15.2.1 Exterior doors: Entrances to the laboratory and vivarium from the exterior of a building shall be controlled and monitored.

- Entrance doors to vivariums shall be UL 752 Level 3 ballistic resistant and 15-minute forced entry resistant.
- Emergency egress doors from laboratory and vivarium spaces shall be controlled and monitored. The door shall be covered by VASS camera (recording only) from the vivarium side and shall be UL 752 Level 3 ballistic resistant and 15-minute forced entry resistant.

5.15.2.2 Interior entry and emergency egress doors: Entrances to the research laboratory and vivarium from other than laboratory or vivarium uses of a building shall be controlled and monitored shall be UL 752 Level 3 ballistic resistant and 15-minute forced entry resistant..

- Emergency egress doors from laboratory and vivarium spaces shall be controlled, monitored, and covered by VASS camera (recording only) from the laboratory or vivarium side.
- Doors to rooms containing select agents shall be controlled and monitored.
- All laboratory and laboratory "neighborhood" doors from public corridors accessible to all building occupants (such as those used for emergency egress) shall be controlled and monitored.
- All doors from public corridors to shared support rooms such as cold rooms, dark rooms, instrument rooms, autoclave rooms, ice machines, and other equipment shall be controlled and monitored.
- Doors to any room used to store radioactive waste, ongoing experiments using radioactive materials, or similar use of radioactive materials shall be controlled and monitored.
- Doors to Irradiator facilities shall be controlled and monitored.
- Entries to the containment area for BSL-3 facilities shall be controlled and monitored.
- Doors from "dirty" corridors to "clean" corridors shall be provided with a sensor and alarm at a central point in the laboratory or vivarium when such door is left open longer than 18 seconds.

5.15.2.3 Elevator entrances: Control of elevator access opening directly into the vivarium shall be by card reader device in the elevator cab, or, where the elevator is dedicated to vivarium use, at any landing from which the elevator can be called. The elevator entrance door at the vivarium shall be monitored by a VASS camera in the space looking at the entrance.

5.15.3 Construction

5.15.3.1 Exterior walls: Construction shall be reinforced masonry, or equivalent. Exterior walls composed of metal or wood frame shall have an interior backing of steel security screen mesh or sheet partition.

- Windows or skylights below 18 feet (4 m) from ground level or the roof of a lower abutment, or less than 18 feet (4 m) from windows of an adjoining building, or accessible by a building ledge leading to windows of other floor rooms, shall have forced entry construction of stainless steel woven security mesh.

5.15.3.2 Interior construction: Interior partitions between the research laboratory and vivarium and surrounding spaces shall be 15-minute forced entry construction and extend from slab to slab.

- All surrounding partitions and walls, floor, and ceiling shall be permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction, to include above the false ceiling and below a raised floor, shall be done in such a manner as to provide visual evidence of unauthorized penetration.
- Partitions and walls surrounding the perimeter of the pharmacy shall be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal shall be spot welded every 6 inches (150 mm) to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.
- Windows or skylights below 18 feet (4 m) from ground level or the roof of a lower abutment, or less than 18 feet (4 m) from windows of an adjoining building, or accessible by a building ledge leading to windows of other floor rooms, shall have forced entry construction of stainless steel woven security mesh.

5.15.3.3 Partitions: Storage rooms containing Category A select agents and irradiator rooms shall be enclosed by 15-minute forced entry-resistant construction as follows.

- Walls, floor, and ceiling shall be permanently constructed and attached to each other.
- All construction, to include above the false ceiling and below a raised floor, shall be done in such a manner as to provide visual evidence of unauthorized penetration.
- Walls shall be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal shall be spot welded every 6 inches (150 mm) to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.

5.15.3.4 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through a perimeter partition shall be protected with either bars or grills. Where one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²), bars are not required; however, all ducts shall be treated to provide sufficient sound attenuation. Where bars are used, they shall be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six inches (150 mm) on center; where grills are used, they shall be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.
- HVAC services shall remain operational 24 hours/day, 7 days/week.

5.15.3.5 Power: Research laboratories and vivaria shall be backed by the standby electrical system. Refer to the VA Electrical Design Manual for specific loads to be connected to the EES.

5.15.4 Security

5.15.4.1 VASS: BSL-3 laboratories and vivariums shall have VASS coverage of internal laboratory spaces which shall be monitored by personnel within the containment area

- VASS cameras shall be placed to monitor any loading dock or other animal receiving area when not already monitored as a part of a general loading/receiving area as provided in this chapter.
- All VASS coverage of access to areas surrounding the containment area shall be monitored in the SCC.

5.15.4.2 Intercom: An intercom shall be provided at each entrance door to a designated office or work station in BSL-3 laboratories or vivariums.

5.15.4.3 Biometric: In conjunction with an access control card reader, a biometric identity verification device shall be provided at the entrance to the ante room. When the biometric device is placed at the door from the ante room to the laboratory, it must be functional for personnel in biosafety garments using contactless method to verify identity (such as, iris or facial recognition not hand geometry or fingerprint device).

5.15.4.4 Access control: Use of other access control systems within the vivarium, including those used for automated watering and/or environmental control and monitoring (such as Edstrom "Watchdog"), shall only be permitted by written authorization of the VA PM with concurrence from the Chief Officer, VHA Office of Research Oversight.

5.15.4.5 Alarms: Provide audible *local alarms* at each door that has an access control device.

5.15.5 Additional Requirements for Select Agent Storage

Facilities handling select agents shall be designed to afford maximum visibility of all areas for observation of use and handling of the select agents.

5.15.5.1 Storage: Storage of select agents (typically in refrigerators and/or freezers) shall be in a separate room.

5.15.5.2 Equipment: Refrigerators and freezers for storage of select agents shall be lockable and covered by VASS (digitally recorded and monitored) placed to allow view of any person accessing the refrigerator or freezer.

5.15.6 Existing Facility – Research Laboratory and Vivarium

Existing laboratories and vivariums in existing facilities shall comply with the requirements of sections 5.15.2, 5.15.3.1 (forced entry security mesh), 5.15.3.5, and 5.15.4.

5.16 Security Control Center

This section addresses the application, monitoring, control, programming, and interface of the Security Control Center (SCC) with all security subsystems: VASS, IDS, PACS, DSPI, and DSS. Additional requirements for the equipment, covered in Chapter 10, should be coordinated with the fundamental planning concepts and criteria associated with the SCC design and security console operating environment covered in this section.

This section supplements the VA Handbook 7610 *Space Planning Criteria*, #279 *Police and Security Service* and VA Handbook 0730 *Security and Law Enforcement* which shall remain in full force and effect.

5.16.1 Adjacencies

The SCC shall be readily accessible to authorized personnel, but shall be inconspicuous and located in areas not frequented by the general public, and shall contain office space, support space, and monitoring equipment that is not visible to unauthorized personnel. The security consultant shall review the proposed location to ensure it is free from other high risk activities.

5.16.1.1 Fire command center (FCC): If a FCC is provided, the SCC shall be adjacent to the FCC, but shall not be accessible to persons using the FCC.

5.16.1.2 Police operations unit: The SCC may be connected to the police operations unit but the two areas shall be served by separate entrances and each area shall be fully functional without requiring access to the other.

5.16.1.3 Back-up SCC: Where provided shall be at a remote location from the primary SCC and meet the requirements of section 5.16.

5.16.1.4 Main lobby: The SCC containing monitoring devices and security personnel shall not be adjacent to the main public lobby.

5.16.1.5 Holding room: The SCC shall not include a holding room.

5.16.1.6 Prohibited adjacencies: The SCC shall not be located closer than 50 feet to a loading dock, emergency department, critical utilities, or other high risk operations or functions.

5.16.2 Entrances

The SCC shall be entered from a corridor beyond the control doors leading out of the lobby to the building interior. The SCC shall have a security vestibule with a *mantrap* configuration. Doors to the SCC shall be UL 752 Level 3 ballistic and 15-minute forced entry rated, controlled, and monitored.

5.16.3 Construction

5.16.3.1 Partitions: The SCC shall be fully enclosed with UL 752 Level 3 ballistic construction and fire resistive construction, including partitions, doors, glazed openings, teller windows, and transaction trays.

- Walls, floor, and ceiling shall be permanently constructed and attached to each other.
- All construction, to include above the false ceiling and below a raised floor, shall be done in such a manner as to provide visual evidence of unauthorized penetration.
- Walls shall be reinforced, slab-to-slab, with 9-gauge expanded metal. The expanded metal shall be spot welded every 6 inches (150 mm) to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.
- Where raised access flooring is used for cable management in the SCC all surrounding partitions shall be built from floor slab to ceiling slab or construction and sealed to an air tight condition.

5.16.3.2 HVAC: All vents, ducts, and similar openings in excess of 96 square inches (620 cm²) that enter or pass through a perimeter partition shall be protected with either bars or grills. Where one dimension of the duct measures less than six inches (150 mm) or duct is less than 96 square inches (620 cm²), bars are not required; however, all ducts shall be treated to provide sufficient sound attenuation. Where bars are used, they shall be 1/2 inch (12.7 mm) diameter steel welded vertically and horizontally six inches (150 mm) on center; where grills are used, they shall be of 9-gauge expanded steel.

- Openings in construction above ceilings or below raised access floors shall be protected as above.
- HVAC serving the SCC shall be independent of the system(s) serving the main lobby.
- The air quality and temperature within the SCC shall allow for a comfortable work environment for both personnel and the security equipment. Ventilation controls shall also be provided on a separate air handling system that provides an isolated supply and return system.
- The SCC shall have a dedicated thermostat control unit and cut-off switch to be able to shut off ventilation to the SCC.

5.16.3.3 Power: The SCC shall be backed by the standby electrical system. Refer to the VA Electrical Design Manual for specific loads to be connected to the EES.

5.16.3.4 Security System Equipment and Interface: The SCC shall be the central point for all monitoring, controlling, programming, and service for all security systems.

Back-up and secondary locations and related security equipment and capabilities shall be identified to support the SCC should it become inoperable. All security subsystems shall be fully integrated by either direct hardwiring of equipment or a computer based electronic Security Management System (SMS). The SCC shall house all attended equipment primary power sources for each security subsystem, such as DVRs, and monitors. Normally unattended equipment, such as servers, shall be located in the main computer room.

- The SCC and security console shall be integrated with field equipment through the proper location, layout, and horizontal and vertical access to designated riser space or secure closets/rooms where the transmission of information from security subsystems will transfer to the SCC. This includes establishing, identifying, and gaining authorized consensus on the use of standalone versus shared space requirements with other telecommunication space.
- Equipment locations, such as wall space for new and upgraded security systems equipment shall be defined in relation to security conduit, power, and panel requirements. Accessibility to areas for installation and security purposes needs to be defined and proximity of these areas to the SCC from an operational efficiency and cost effective perspective shall be addressed.
- All equipment that is rack mounted or installed in a security console shall be clearly labeled as to its identification. Labeling, such as in the case of VASS monitors, may be programmed with a message embedded or programmed on the monitoring screen.

5.16.4 Physical Security

The SCC shall have physical security safeguards. The main entry door shall have a card reader or biometric security credential device for authorized personnel and an intercom or similar device for unauthorized persons to request assistance. Provide a fixed VASS camera connected to a dedicated monitor within the SCC for direct communications and visual verification of the person using the intercom. Remote unlocking of the door shall be prohibited.

5.16.5 Primary and Secondary Locations

The SCC shall be located in an area that is within the first level of security defense defined by VA. The SCC shall also be located above grade and above any potential flood areas, such as basement.

5.16.5.1 Location: The SCC shall be located in an area free of background noise influences that could impact equipment and SCC operations. To prevent potential compromise of operations, staff health, and safety, the SCC shall be located away from exterior building walls that are adjacent to roadway traffic, parking, and air intake areas and facility utility, environmental, and operational areas, that if compromised, damaged, or destroyed, could impact SCC operations.

5.16.5.2 Secondary SCC: A secondary or backup SCC shall be established in another building or location within the same facility that is far removed from the primary SCC. The secondary SCC shall be provided with full redundancy of the electronic security

systems and associated security console operations. The security technology shall be designed and engineered to provide flexibility to monitor and operate security subsystems from remote and multiple facility locations and security workstations.

5.16.6 Space Requirements

The size of the SCC shall be defined by the number of console bays required to house and operate the security subsystems and provide adjacency to the VA Police operations area which includes offices, meeting and training rooms, armory, and holding room. The SCC shall meet UFAS requirements to provide accessibility to the security console, to access equipment and wiring, console pull-out trays and doors, telephones, master intercom stations, base radio communications, and computer terminals. Floor area planning decisions will depend upon the number of console positions, size of the facility, and overall architecture of the ESS. Centralized architecture, where all video recording is located within the security equipment room (SER), will require additional space versus decentralized architecture. As a general rule, the SER will be a minimum of 50 percent of the overall SCC size, at a minimum 9 feet x 10 feet (3 m x 3 m) for a small SCC. Future expansion of the SCC and security console equipment requirements shall be addressed and may be accommodated through use of modular furniture.

5.16.6.1 Configuration: The SCC shall have two core spaces, the SCC itself and the security equipment room (SER). The SCC shall consist of a monitoring function (ESS monitors, communications devices, fire alarm, etc.). The SER shall consist of supportive equipment (video storage devices, data transmission systems/media, etc.) that is not monitored. Servers shall be located within the main computer room.

- **Security equipment room (SER)** shall serve as the supporting equipment room for the SCC and shall be designed with sufficient space to accommodate 100 percent system growth. The SER layout shall follow BISC standards for room layout (Telecommunication Room). Computer racking shall be centered in the room, permitting access doors to be opened on all sides. Maintain minimum required electrical code distances from the UPS and wall-mounted enclosures and devices.
- **Security equipment closet (SEC)** shall follow VA OIT Design Standards and share space in the Telecommunication Room. SEC shall have a defined space and shall be physically separated per the OIT standard. Where security equipment will be wall mounted, a 0.75 inch (19 mm) fire-rated plywood (or comparable material) shall cover the wall. Where security equipment will be rack mounted, provide securable security equipment cabinets. All incoming and outgoing conduit shall terminate/originate at metal wire troughs mounted above the security equipment cabinets or racks. All equipment mounting conditions shall include dedicated horizontal and vertical wire and cable management systems.

5.16.6.2 Small SCC: A small SCC shall contain no more than four security console bays. 150-300 square feet of space shall be provided for a small to medium size SCC operation. The small SCC is commonly associated with facilities or campuses with facilities between 150,000 to 300,000 GSF. The SER shall be not less than half the size

of the SCC and no smaller than 90 square feet. Facilities smaller than 150,000 GSF shall be monitored by the VISN SCC.

5.16.6.3 Large SCC: A large SCC shall contain no less than five and no more than eight security console bays. For large SCC operating environments, 500 square feet of space shall be provided. The SER shall be not less than half the size of the SCC and no smaller than 180 square feet.

5.16.6.4 Back-up or secondary SCC: Area requirements for a back-up SCC shall be based on what ESS systems will be monitored.

5.16.7 Operational Requirements

The SCC shall provide continuous and consistent monitoring, surveillance, response, and operation of security subsystems.

5.16.7.1 Security Console/Workstation: The SCC security console may use stand-up, sit-down, and vertical equipment racks in any combination to monitor and control the security subsystems.

- The console shall be ergonomically designed with efficient writing and storage space provided and all security equipment requiring repetitive interaction and response by the console operator shall be easily accessed, observed, and accomplished.
- All console bays and equipment racks shall be made of metal, furnished with wire ways, power strips, thermostatic controlled bottom or top mounted fan units (coordinate with space and rack cooling plan), a hinge mounted rear door, front hinged door of Plexiglas, and a louvered top. In addition, space shall be provided for telephones, master intercom units, portable base station radio unit, computer monitors, and printers.
- All console bays shall be mounted on lockable casters and all console wiring shall be neatly organized, labeled, and made easy to access.

5.16.7.2 Accessibility: The SCC shall be fully accessible to persons with disabilities.

5.16.8 Existing Facility – Security Control Center (SCC)

Where the existing SCC does not meet the requirements of section 5.16, a secondary SCC that complies with the requirements of section 5.16.5.2 shall be provided.

6 BUILDING ENVELOPE

6.0 Scope, Purpose, and Goals

This section provides requirements for exterior walls other than load bearing walls; glazed façade fenestration and glazed atria; for roof structures, including skylights; and air intakes and exhausts servicing critical equipment but does not pertain to stacks and wall openings for non-critical equipment. These requirements are in addition to the requirements for conventional façade design, including the provisions for hurricane, earthquake, and any other extreme loading condition required by code. The magnitudes of W1 and GP2 are defined in the Physical Security Design Standards Data Definitions, a document separate from this Manual. It is provided on a need-to-know basis to the blast/structural engineers performing analysis and design of VA projects. Authorized users can contact the Office of Construction and Facilities Management (CFM) in VA to request the document. [Note: The W and GP values in the Physical Security Design Standards Data Definitions were updated along with this Manual. Users shall use the updated values.]

Connecting corridor concourse and bridges, that are not the main entrance or required exit for the connected buildings, and freestanding greenhouses shall be exempt from the requirements of Chapters 6 and 7. When the connecting corridor or bridge includes the main entrance for the connected buildings, it shall not be exempt. When the internal wall is shared with a VA mission critical facility, the internal wall is to be designed as an exterior wall per the requirements of Chapter 6 and Chapter 7. Physical security requirements for temporary buildings shall be determined on a case by case basis by the AHJ.

In order to meet the physical security standards of this chapter, the design team must include a security specialist and a structural blast specialist. The qualifications requirements for these specialists are included in section 1.5.

6.1 Walls

6.1.1 Non-load Bearing Walls

Non-load bearing walls shall be designed such that they have some permanent deformation but are generally repairable in response to the calculated peak pressures and impulses resulting from the design level vehicle threat (W1) located at the minimum standoff distance of 50 feet (15 m), but no greater than GP2. Standoff provided in excess of the 50 feet (15 m) or increased distances over the height of the building may not be accounted for in the calculation of the blast loading environment. Although negative phase loading should not be considered, the effects of rebound shall be included in the design of blast resistant façade. Deformations shall be as defined by the B2 response limits per the Protective Design Center document PDC-TR 06-08, *Single Degree of Freedom Structural Response Limits for Antiterrorism Design*.

6.1.1.2 Supporting structure: Walls shall span from slab to slab and shall not be attached directly to gravity load bearing elements (such as columns and shear walls)

unless an advanced analysis of the load bearing element demonstrates it can accept the maximum blast forces transferred by the members framing into it without compromising its load bearing capacity.

6.1.1.3 Loads: Walls shall be able to accept the tributary loads transferred from glazed fenestration in addition to the design level blast pressures applied directly to their surface.

6.1.2 Existing Facility – Walls

For building upgrades in which the façade is being completely replaced, the existing facility shall comply with the requirements defined in Section 6.1.1.

6.2 Fenestration and Doors

6.2.1 Façade Fenestration

All façade fenestration shall be designed to crack but remain in the frame in response to the calculated peak pressures and impulses resulting from the design level vehicle threat (W1) located at minimum standoff distance of 50 feet (15 m), but no greater than GP2. Standoff provided in excess of the 50 feet (15 m) or increased distances over the height of the building may not be accounted for in the calculation of the blast loading environment. Although negative phase loading should not be considered, the effects of rebound shall be included in the design of blast resistant glazing. All blast resistant design requirements are in addition to the requirements of the VA Window Specifications. The use of operable windows for blast resistant design is discouraged; however, where operable windows are required, their performance must be demonstrated with acceptable explosive (or shock tube) test data while in the open position.

6.2.1.1 Glass: All new exterior glazing is to use laminated glass. For insulated glazing units (IGUs) the laminated glass is required only for the inner lite.

6.2.1.2 Glazing: The glass shall be restrained within the mullions with a minimum ½" bite and a continuous bead of structural silicone adhesive attaching the inner lite of glass to the frame to allow it to develop its post-damage capacity.

6.2.1.3 Mullions: The mullions are to be of aluminum and/or steel construction and shall be designed to accept a blast load equal to the maximum capacity of the weakest lite of supported glass (i.e., *balanced design*), but no less than the design level pressures while sustaining deformations no greater than L/60. For windows with glazing lay-up governed by non-blast requirements (hurricane, forced entry, fabrication, handling, and ballistic), mullions are to be designed for the capacity of the glazing that would be required to meet the blast requirements only.

6.2.1.4 Curtainwall: Curtainwall framing members shall span from slab to slab and shall not be attached directly to gravity load bearing elements (such as columns and shear walls) unless an advanced analysis of the load bearing element demonstrates it can accept the maximum blast forces transferred by the members framing into it without compromising its load bearing capacity.

6.2.2 Existing Facility – Fenestration

For upgrades in which the façade is not replaced, a mechanically anchored or wet glazed attached 7-mil thick anti-shatter film may be used to satisfy the requirements of this section. Glass replacement upgrades, window replacement upgrades, and “storm-window” upgrades interior to existing historic facade shall use laminated glass and structural silicone sealant. For insulated glazing units (IGUs) the laminated glass is required only for the inner lite. No upgrades to the frames or mullions are required for glass replacement projects. For upgrades in which the façade is being completely replaced, the existing facility shall comply with the requirements defined in Section 6.2.1.

6.2.3 Doors

All doors shall be designed using debris mitigating materials such as laminated glass and heavy gauge metal (14-gauge minimum), shall open towards the detonation, and the heavy duty frames and anchorages shall be capable of resisting the collected blast loads. Frame rotations shall be limited to L/60.

All roll down doors shall be constructed of 14-gauge metal, and the anchorage to the overhead support shall be designed to resist the collected blast loads.

6.3 Atria

6.3.1 Atria

All vertical, horizontal, and sloped glass surfaces shall be designed to crack and remain in the frame in response to the calculated peak pressures and impulses resulting from the design level vehicle threat (W1) located at the minimum standoff distance of 50 feet, but no greater than GP2. Standoff provided in excess of the 50 feet (15 m) or increased distances over the height of the building may not be accounted for in the calculation of the blast loading environment. Although negative phase loading should not be considered, the effects of rebound shall be included in the design of blast resistant façade. All blast resistant design requirements are in addition to the requirements of the VA Window Specifications.

6.3.1.1 Skylights: See section 6.4.2.

6.3.1.2 Glass: See Section 6.2.1.1.

6.3.1.3 Glazing: See Section 6.2.1.2.

6.3.1.4 Mullions: See Section 6.2.1.3.

6.3.1.5 Framing: Atria framing members shall be designed to continue carrying gravity loads while sustaining deformations no greater than L/60 in response to the collected blast loads.

6.3.2 Existing Facility – Atria

Upgrades involving the replacement of the atria framing shall meet the requirements of section 6.3.1.5.

6.4 Roofs

6.4.1 Roof Structure

Roof structure (including metal deck, composite deck, concrete slabs, beams, joists, and girders) shall be designed to withstand the calculated peak incident pressures and impulses resulting from the design level vehicle threat (W1) located at the minimum standoff distance of 50 feet (15 m). Note that the GP2 peak pressure and impulse limit should not be used in the design of the roof structure. Standoff provided in excess of the 50 feet (15 m) may not be accounted for in the calculation of the blast loading environment. Although negative phase loading should not be considered, the effects of rebound shall be included in the design of blast resistant roof. Deformations shall be as defined by the B2 response limits per the Protective Design Center document PDC-TR 06-08, *Single Degree of Freedom Structural Response Limits for Antiterrorism Design*. The blast loading shall take into account the presence of parapets, the diffusion of blast waves, and the spatial extent of the roof surface.

6.4.2 Skylights

Skylight glass shall be designed to crack but remain in its frame in response to the calculated peak pressures and impulses resulting from the design level vehicle threat (W1) located at the minimum standoff distance of 50 feet (15 m), but no greater than GP2. Standoff provided in excess of the 50 feet (15 m) may not be accounted for in the calculation of the blast loading environment.

6.4.2.1 Glass: All skylight glazing is to use laminated glass. For insulated glazing units (IGUs) the laminated glass is required only for the inner lite.

6.4.2.2 Glazing: Skylight glass shall be restrained within the mullions with a minimum ½" bite and a continuous bead of structural silicone adhesive attaching the inner lite of glass to the frame, to allow it to develop its post-damage capacity.

6.4.2.3 Mullions: The mullions are to be of aluminum and/or steel construction and shall be designed to accept a blast load equal to the maximum capacity of the weakest lite of supported glass (i.e., balance design), but no less than the design level pressures while sustaining deformations no greater than L/60.

6.4.3 Penthouses Enclosing Critical Equipment

Penthouse enclosures shall be designed to resist the peak blast pressures and impulses resulting from the design level vehicle threat (W1) located at the minimum standoff distance of 50 feet (15 m), but no greater than GP2. Standoff provided in excess of the 50 feet (15 m) may not be accounted for in the calculation of the blast loading environment.

6.4.4 Existing Facility – Roofs

For upgrades in which the skylight is not replaced, a mechanically anchored or wet glazed 7-mil thick anti-shatter film may be used to satisfy the requirements of this section. Glass replacement upgrades shall use laminated glass and structural silicone sealant. For insulated glazing units (IGUs) the laminated glass is required only for the inner lite. No upgrades to the frames or mullions are required for glass replacement projects. For upgrades in which the skylight roof is being completely replaced, the existing facility shall comply with the requirements defined in Section 6.4.2. For upgrades in which the structural roof is being completely replaced the existing facility shall comply with the requirements defined in Section 6.4.1.

6.5 Air Intakes and Exhausts Servicing Critical Equipment

6.5.1 Intakes and Exhausts

Air intakes and exhausts shall be designed to minimize the blast over pressure applied to critical mechanical equipment due to the design level vehicle threat (W1) located at the minimum standoff distance of 50 feet (15 m) by means of hardened plenums and internal or external structured baffles. Standoff provided in excess of the 50 feet (15 m) may not be accounted for in the calculation of the blast loading environment. Deformations of hardened plenums and structured baffles in response to the blast loading shall be as defined by the B3 response limits per the Protective Design Center document PDC-TR 06-08, *Single Degree of Freedom Structural Response Limits for Antiterrorism Design*. Anchorage of baffles shall be designed for the collected blast loads. Baffles shall provide an overlap that is equivalent to the space between the baffle and the surrounding wall. The design shall deny a direct line of sight from the design level vehicle threat (W1) located at the standoff distance to the critical infrastructure within. Where direct lines of sight cannot be denied, distributed redundancy may be required to provide continuous operations. Louvers in areas prone to hurricanes or wind hazards (in accordance with ASCE 7-10) shall be certified by the manufacturer to meet the following Florida Building Code tests: Uniform Static Air Pressure Test, Cyclic Wind Pressure Test, Large Missile Impact Test, and Wind Driven Rain Resistance Test.

6.5.2 Existing Facility – Air Intakes and Exhausts Servicing Critical Equipment

Air intakes and exhausts shall be upgraded to minimize the extent of debris that may enter *critical spaces* in response to the design level vehicle threat (W1) located at the minimum standoff distance of 50 feet (15 m). Standoff provided in excess of the 50 feet (15 m) may not be accounted for in the calculation of the blast loading environment. Hardened plenums and structured baffles, impact and wind driven rain resistant louvers, as described in section 6.5.1, shall be installed when a major interior renovation or major equipment replacement is performed.

6.6 Calculation Methods

All blast design and analysis, whether for new or existing construction, shall be performed in accordance with accepted methods of structural dynamics. Explosive (or shock tube) testing is required wherever operable windows are used or where the behavior of energy absorbing or other complex façade systems cannot be characterized by analytical methods.

6.6.1 Design and Detailing

The performance of façade in response to blast loading is highly dynamic and often inelastic. Design and detailing of protected façade shall therefore be based on analytical methods that accurately represent the loads and response. Explosive test data, developed by an experienced testing facility approved by the U.S. Government (USG), may be used to supplement the analytical methods where a direct analytical representation is not feasible.

6.6.2 Blast Loads

Blast loads shall typically be developed using the semi-empirical relations of UFC 3-340-01, *Design and Analysis of Hardened Structures to Conventional Weapons Effects*, dated June 2002 (CONWEP).

6.6.3 Dynamic Response

Dynamic structural response analyses shall be performed using either empirical data developed by an approved USG testing laboratory, simplified Single-Degree-of-Freedom (SDOF) analytical methods or advanced Finite Element Methods (FEM). Where simplified SDOF methods are used, the performance criteria shall be in accordance with this document. Where advanced FEM are used, the performance shall be demonstrated through interpretation of the calculated results. Dynamic glass response analyses shall be performed using window glazing analysis and design software developed by the USG, such as WINGARDPE, WINLAC, or HAZL, which are capable of predicting the glass, film, and laminate response when subjected to the blast loading environment.

7 STRUCTURAL SYSTEM

7.0 Scope, Purpose, and Goals

This chapter provides requirements for blast resistant structures and includes requirements for the prevention of progressive collapse and the hardening of critical columns and load bearing walls. All building components requiring blast resistance must be designed using established methods and approaches for determining dynamic loads, structural detailing, and dynamic structural response. Alternative analysis and mitigation methods are permitted, provided that the performance level is attained.

While structural hardening makes the structure resistant to a specific threat, design to resist progressive collapse increases the robustness of the structure to an undefined event. This threat independent approach provides redundant load paths, ductility, and continuity. Designers may apply static and/or dynamic methods of analysis to demonstrate compliance with this requirement.

These requirements are in addition to the requirements for conventional structural design, including the provisions for hurricane, earthquake, and any other extreme loading condition required by code. The magnitudes of W1 and W2 are defined in the Physical Security Design Standards Data Definitions, a document separate from this Manual. It is provided on a need-to-know basis to the blast/structural engineers performing analysis and design of VA projects. Authorized users can contact the Office of Construction and Facilities Management (CFM) in VA to request the document. [Note: The W and GP values in the Physical Security Design Standards Data Definitions were updated along with this Manual. Users shall use the updated values.]

The minimum physical requirements for the construction of active and passive vehicle barriers are also included in this chapter.

Connecting corridor concourse and bridges, that are not the main entrance or required exit for the connected buildings, and freestanding greenhouses shall be exempt from the requirements of Chapters 6 and 7. When the internal wall is shared with a VA mission critical facility, the internal wall is to be designed as an exterior wall per the requirements of Chapter 6 and Chapter 7. Physical security requirements for temporary buildings shall be determined on a case-by-case basis by the VA PM with concurrence of the AHJ.

In order to meet the physical security standards of this manual the design team must include a security specialist and a structural blast specialist. The qualifications for these specialists are included in section 1.5.

7.1 Blast Resistance

Structures shall be constructed to withstand the actual pressures and corresponding impulses produced by the design level vehicle threat (W2) located at the minimum standoff distance of 50 feet (15 m) and the design level satchel threat (W1) that may be delivered to loading docks, mailrooms, and lobbies. Standoff distances provided in excess of the 50 feet (15 m) may not be accounted for in the calculation of the blast loading environment.

The design shall provide a level of protection for which progressive collapse will not occur, the building damage will be economically repairable, and the space in and around damaged area can be used and will be fully functional after cleanup and repairs.

7.1.1 Priority for Protection

The priority for blast resistance shall be given to critical elements that are essential to mitigating progressive collapse. Designs of secondary structural elements, primary nonstructural elements, and secondary non-structural elements shall minimize injury and damage. The priority depends on the relative importance of structural or non-structural elements in the following order.

All flexural elements and their connections shall be designed and detailed such that no brittle failure mode limits the capacity of the section. Unless the element is designed to remain elastic in response to blast loading, ductile failure modes shall be the governing failure mode for flexural elements and their connections and splices. When the elements are designed to resist the blast loads elastically, the design of non-ductile modes shall include a 1.5 factor of safety on the calculated forces.

7.1.1.1 Primary structure: Primary structural elements are the essential parts of the building's resistance to catastrophic failure, including columns, girders, roof beams, and the main lateral resistance system. Deformations shall be as defined by the B1 response limits per the Protective Design Center document PDC-TR 06-08, *Single Degree of Freedom Structural Response Limits for Antiterrorism Design*.

7.1.1.2 Secondary structure: Secondary structural elements are all other load bearing members, such as floor beams and slabs. Deformations shall be as defined by the B2 response limits per the Protective Design Center document PDC-TR 06-08, *Single Degree of Freedom Structural Response Limits for Antiterrorism Design*.

7.1.1.3 Primary non-structural (non-façade elements): Primary non-structural elements and their attachments that are essential for life-safety systems or elements that can cause substantial injury if failure occurs, including overhead heavy suspended mechanical units or fixtures weighing more than 31 lbs. Anchor these elements (excluding distributed systems such as suspended ceilings or piping networks) with lateral ties capable of resisting lateral motions associated with the building's calculated blast induced base shear. This requirement does not preclude the need to design the mountings for forces required by other criteria such as seismic standards.

7.1.1.4 Secondary non-structural: Secondary non-structural elements are all elements not covered in primary non-structural elements, such as partitions, furniture,

and light fixtures. Provide a positive means of attachment of these elements to the building structure and to designing arrangements that will minimize debris following in-structure shock motions.

7.1.2 Existing Facility – Blast Resistance

See section 7.3.1.

7.2 Progressive Collapse

Single story structures are exempt from progressive collapse requirements. Two story structures shall be designed to minimize the potential for progressive collapse using the Tie Force Method in which the structure shall develop peripheral, internal, and vertical tie forces by providing continuous reinforcement and ductile detailing. All structures, greater than two stories, shall be designed to minimize the potential for progressive collapse using the Tie Force Method, enhanced local resistance and the Alternate Path Method, which requires the structure to withstand the threat independent removal of any exterior column, one at a time, or one bay width of exterior load bearing walls, one at a time, without precipitating a disproportionate extent of damage. Consideration shall be given to ductile moment resisting frame lateral systems at the exterior of the building. The requirements of the Tie Force Method, enhanced local resistance, and alternate path analysis methods for demonstrating a structure's resistance to progressive collapse shall conform to U.S. Government (USG) guidelines, specifically, Design of Buildings to Resist Progressive Collapse, UFC 4-023-03 dated 27 January 2010. All exterior columns, including columns within open courtyards shall be designed to prevent progressive collapse. Closely spaced columns, closer than 30 percent of the largest bay dimension, are to be removed in the same alternate path analysis.

7.2.1 Existing Facility – Progressive Collapse

No additional physical security requirements.

7.3 Column Protection

Columns and load bearing walls exposed to blast loading shall be hardened or isolated to resist the effects of the design level vehicle threat (W2) located at the provided standoff distance and the design level satchel threat (W1) that may be delivered to loading docks, mailrooms, and lobbies prior to screening. The design shall provide a level of protection for which progressive collapse will not occur, the building damage will be economically repairable, and the space in and around damaged area can be used and will be fully functional after cleanup and repairs. Deformation limits shall be as defined by the B2 response limits per the Protective Design Center document PDC-TR 06-08, *Single Degree of Freedom Structural Response Limits for Antiterrorism Design*.

7.3.1 Existing Facility – Column Protection

Protect columns in spaces the public can access prior to screening from explosive devices by installation of architectural or structural finishes that prevent detonation within 6 inches (152 mm).

7.4 Wall Protection

Non-load bearing interior walls separating high risk interior spaces (loading docks, mailrooms, and lobbies) shall be hardened to resist the effects of the design level satchel threat (W1) that may be delivered to these spaces. Walls shall be of reinforced masonry or concrete construction. Deformation limits shall be as defined by the B2 response limits per the Protective Design Center document PDC-TR 06-08, *Single Degree of Freedom Structural Response Limits for Antiterrorism Design*. Doors within these walls are to be of heavy gauge steel or laminated glass construction and are to open into the high risk space.

7.4.1 Screen Walls

Non-load bearing screen walls that enclose critical equipment and the structure providing lateral resistance shall be hardened to withstand the actual pressures and corresponding impulses produced by the design level vehicle threat (W2) located at the minimum standoff distance of 50 feet (15 m). Walls shall be of reinforced masonry or concrete construction. Deformation limits shall be as defined by the B3 response limits per the Protective Design Center document PDC-TR 06-08, *Single Degree of Freedom Structural Response Limits for Antiterrorism Design*. Doors within these walls are to be of heavy gauge steel and are to open outwards.

7.5 Anti-ram Resistance

7.5.1 Vehicle Barriers

Both active and passive barriers shall be tested and certified to be capable of stopping a 4,000 pound (1,800 Kg) vehicle at a speed of 30 miles per hour (48 Km/hr) with a maximum penetration distance of 3.3 feet (1m). (See also Chapter 3, Section 3.4 Vehicle Barriers.)

7.5.1.1 Certification/Testing: Performance of anti-ram element shall be demonstrated by means of impact testing or detailed finite element analysis of the vehicle impact. Testing is to be performed using either ASTM 2656-07 or DOS SD-STD-02.01, Revision A.

7.5.1.2 Active barriers: Active barriers shall be electric or hydraulic wedges, bollards, beams, drop arms, or sliding gates.

7.5.1.3 Passive barriers: Passive barriers shall be walls, stationary bollards, cables, or combination of landscape and hardscape that achieves the required anti-ram resistance.

7.5.2 Existing Facility – Anti-ram Resistance

The requirements of section 7.5.1 shall apply.

7.6 Calculation Methods

All blast design and analysis, whether for new or existing construction, shall be performed in accordance with accepted methods of structural dynamics.

7.6.1 Design and Detailing

The performance of structures in response to blast loading is highly dynamic and often inelastic. Design and detailing of these structures shall therefore be based on analytical methods that accurately represent the loads and response. Explosive test data, developed by an experienced testing facility approved by the USG, may be used to supplement the analytical methods where a direct analytical representation is not feasible.

7.6.2 Blast Loading

Blast loads shall typically be developed using the semi-empirical relations of UFC 3-340-01 (CONWEP); however, where near contact detonations are considered, Computational Fluid Dynamics (CFD) methods may be required.

7.6.3 Dynamic Response

Dynamic structural response analyses shall be performed using either empirical data developed by an approved USG testing laboratory, simplified Single-Degree-of-Freedom (SDOF) analytical methods, or advanced Finite Element Methods (FEM). Where simplified SDOF methods are used, the performance criteria shall be in accordance with this section. Where advanced FEM are used, the performance shall be demonstrated through interpretation of the calculated results.

8 UTILITIES & BUILDING SERVICES

8.0 Scope, Purpose, and Goals

This chapter describes criteria for site utility entrances (services), onsite utility distribution, and building services. Utility systems include but are not limited to, potable and industrial water, fire protection water, sanitary sewer, fuels, steam, chilled water, electrical power, and telecommunications. Site utility entrances may include utility-owned service and metering equipment. Utility services shall be designed in accordance with VA Design Manuals including the Electrical, HVAC, Plumbing, Fire Protection, Outside Steam Distribution, and Sanitary Design Manuals. In addition, equipment and services required to keep a mission critical facility in operation shall not be located in high risk areas.

8.1 Utility Entrances

8.1.1 Mechanical

8.1.1.1 Alternate connections for steam and chilled water: Provide means for the connection of an alternate source, such as a mobile boiler, chiller, or cooling tower.

8.1.1.2 Water service: Provide a minimum of two full demand water service connections to the campus fed from either separate sources (if cost effective) or two separate connections to a single multi-sourced network. Full demand includes potable, industrial and fire protection water. Services connections shall enter the campus at separate locations through separate isolation valves. The purpose of this provision is to provide an uninterrupted supply of potable water or permit swift service restoration in the event of a water main break or contamination of one source. If two separate water connections as described are not reasonably available for an outside provider, an onsite source, such as a water well with treatment means, shall serve as the second source. . See section 8.4 for onsite water storage requirements.

8.1.1.3 Protection of utility-owned service equipment: Above-ground utility owned service equipment shall be located above the 100-year floodplain, above grade, and within a mission critical building envelope, when possible, or be protected by limited-access masonry enclosures and be located a minimum of 50 feet (15 m) in all directions from high-risk areas. Coordinate with the serving utility.

8.1.2 Electrical

8.1.2.1 Number of services: Two utility services are required. Services shall be from separate utility substations, when the availability of utility sources permits.

8.1.2.2 Separation of services: Electric service feeders shall be underground, located away from other utility services, and located away from high-risk areas. Services shall be separated by a minimum distance of 50 feet (15 m) where possible.

8.1.2.3 Protection of utility-owned service equipment: Utility-owned service and metering equipment shall be located above the 100-year floodplain, above grade, and

within a mission critical building envelope, when possible, or be protected by limited-access masonry enclosures and be located a minimum of 50 feet (15 m) in all directions from high-risk areas. Coordinate with the serving utility.

8.1.3 Telecommunications

8.1.3.1 Number of services: Two services from each telecommunications provider are required, preferably with delivery from different central offices or sites.

8.1.3.2 Separation of services: Telecommunications cable pathways shall be underground, located away from other utility services, and located away from high-risk areas. Where more than one service is obtained, services shall be separated by a minimum distance of 50 feet (15 m).

8.1.3.3 Redundant service paths to demarc: The *demarc* is the separation point between utility-owned and VA-owned equipment. Telecommunications cable pathways shall be designed to provide redundant services to the demarc from the street or property line where the interface with the service provider takes place. Redundant conduit paths shall be separated by a minimum distance of 50 feet (15 m).

8.1.4 Existing Facility – Utility Entrances

8.1.4.1 Existing facilities shall comply with the redundancy requirements of section 8.1.

8.1.4.2 Relocate existing mechanical and electrical equipment to comply with section 8.1. Where existing equipment cannot be relocated to within an existing building envelope, protect the equipment with screen walls or barriers that comply with Chapters 6 and 7.

8.2 Site Distribution

8.2.1 Mechanical

8.2.1.1 Steam, chilled water, water, and fuel system distribution: Distribution systems shall be underground and shall be looped systems, such that an interruption at any one point can be isolated and service maintained to the facility. Piped utility systems, in particular fuel systems, shall include enhanced capability to resist external forces. Steam and condensate piping shall be installed above grade and not be located in high risk areas.

8.2.1.2 Separation of sanitary sewer and storm drain systems: Sanitary sewer and storm drain systems shall be separate.

8.2.1.3 Manhole and handhole covers: Manholes and handholes shall be equipped with lockable covers.

8.2.2 Electrical

8.2.2.1 Separation of feeders: Feeders that form a primary selective pair shall not be located closer than 50 feet (15 m) to each other, shall be installed in concrete-encased ductbanks, and shall enter served buildings at different locations. Feeder entry points will maintain a minimum distance of 50 feet (15 m) or greater in all directions from areas such as loading docks or similar defined areas of vulnerability.

8.2.2.2 Location of distribution equipment: All electrical distribution components, such as medium- and low-voltage switchgear and transformers, shall be located above the 100-year floodplain, above grade, and within a mission critical building envelope. Pad-mounted outdoor electrical equipment is not permitted.

8.2.2.3 Manhole and handhole covers: Manholes and handholes shall be equipped with lockable covers.

8.2.3 Telecommunications

8.2.3.1 Telecommunications systems distribution: An underground ring topology shall be used for telecommunications cable pathways that connect multiple buildings. This will provide two underground pathways for telecommunications services to all buildings. Sizing of conduits shall be based on a 40 percent fill, and there will be a minimum of two spare four inch (100 mm) conduits between buildings. Conduits shall be encased in concrete. Distance between manholes or handholes shall not be greater than 400 feet (122 m).

8.2.3.2 Separation of pathways: Ring distribution pathways shall not be located closer than 50 feet (15 m) to each other. Pathways shall enter served buildings at different locations and shall not be exposed on the building exterior. Quantity and size of conduits shall be determined by site design. Telecommunications entry points shall maintain a minimum distance of 50 feet (15 m) or greater in all directions from areas such as loading docks or similar defined areas of vulnerability.

8.2.3.3 Location of telecommunications equipment: All telecommunications components other than inter-building cabling shall be located above the 100-year floodplain, above grade, and within a mission critical building envelope.

8.2.3.4 Manhole and handhole covers: Manholes and handholes shall be equipped with lockable covers.

8.2.4 Existing Facility – Site Distribution

8.2.4.1 Existing facilities shall provide emergency connections for electricity, steam, and all water systems.

8.2.4.2 Where existing outdoor above-ground distribution equipment cannot be relocated to within an existing building envelope, protect the equipment with screen walls or barriers that comply with Chapters 6 and 7.

8.3 Energy Center

8.3.1 Requirements

The energy center contains utility production and distribution equipment, as well as incoming services from offsite utility providers, and is responsible for providing utility services during normal operating conditions as well as during and after natural and manmade disaster events. The utility services feeding into the energy center include but may not be limited to electricity, potable water, natural gas, and fuel oil. The utilities feeding to and/or from the energy center and the mission critical facility shall be electricity, steam and condensate return, and chilled water supply and return.

8.3.2 Sustained Service

The energy center shall sustain utility services for a minimum time period of 96 hours.

8.3.3 Standby Electrical System

Refer to 9.2.1 Standby Electrical System.

8.3.4 Long-replacement-time Equipment

For equipment that has a long replacement time, provide for additional physical protection and/or installation of redundant equipment or connections that will alleviate extended shutdown time.

8.3.5 Existing Facility – Energy Center

Existing facilities shall comply with the requirements of sections 8.3.2 and 8.3.3.

8.4 Water and Fuel Storage

Designers shall base the water and fuel storage needs on the number of people anticipated to be on the site during an event. This shall include all mission critical facilities and those life safety protected facilities that are anticipated to remain operational.

Background: The director of a mission critical facility, in consultation with the area emergency manager, shall provide an estimate of the total number of people expected to be on the site, including patients or residents, staff, family members (of patients, residents, and staff), visitors, and potential “refugees.” Standards of the Joint Commission (TJC) require hospitals to address the provision of water and utilities as part of the facility’s Emergency Operations Plan (EOP). TJC requires that the EOP state how a hospital will manage utilities during an emergency. In accordance with TJC, the EOP identifies the hospital’s capabilities and establishes response procedures for when the hospital cannot be supported by the local community in the hospital’s efforts to provide communications, resources and assets, security and safety, staff, utilities, or patient care for at least 96 hours. Additional VA guidance is provided in [The Emergency Management Program Guidebook](#)³, published by VHA’s CEOSH, and states the “TJC does not require facilities to stockpile 96-hours of supplies, but to develop a concept of operations. It is important to realize that an

appropriate response may involve closing or evacuating the health care organization after a certain period. For example, an organization may determine that it can be self-sufficient during an emergency for 48 hours after which point it will initiate evacuation procedures."

8.4.1 Requirements

Storage shall be provided for potable and industrial water, fire protection, wastewater, and contaminated water, and fuels for use during the period under which offsite utilities are unavailable. At a minimum, water and generator fuel storage shall support 96 hours of operation, and boiler fuel storage shall support 10 January days of operation.

Note: The potable water system shall meet the requirements of VHA Directive 2006-007 Ensuring the Security and Availability of Potable Water at VHA Facilities (February 6, 2006).

8.4.2 Storage Volume Criteria:

This section provides the basis of design for all new construction and major renovation projects involving mission critical building(s) and corresponding sites. Consistent with the guidance of Section 1.9, any site where a new or renovated mission critical facility is to be constructed, the entire site shall be upgraded to conform to these standards. When the entire site cannot be upgraded to meet this criteria, the project shall be designed to incorporate achievable physical security elements in a manner that will allow enhancement of those elements in the future. Future project(s) must be included in the facility's approved Strategic Capital Investment Plan (SCIP). Designers can adjust potable and industrial water storage criteria only under the following conditions and with approval from the Facility Director and Project Manager:

- The possibility of natural disasters such as hurricanes, earthquakes, flooding and fire dictate an increase in the storage volume requirements.
- Potable and industrial water storage may be reduced if a water conservation strategy is developed and approved by the Facility and VISN Directors in an Emergency Water Supply Plan (EWSP). The EWSP must be approved in writing at the time of project conceptual design.

Note: To guide facility managers in the assessment of water storage needs, the Department of Health and Human Services along with The Centers for Disease Control and Prevention, and the American Water Works Association published the Emergency Water Supply Planning Guide for Hospitals and Health Care Facilities. The objective of this guide is to help health care facilities develop a robust EWSP and provides a detailed methodology for identifying: current water use, minimum water needs, emergency water conservation measures and alternative water supplies. Directors of Mission Critical facilities along with project designers shall develop a EWSP when designing for less emergency water storage than stipulated in Section 8.4.1. The resulting EWSP shall be included in the project's basis of design and the hospital EOP.

8.4.2.1 Water and Waste-Water: Minimum criteria to be used in determining storage requirements are:

8.4.2.1.1 Potable water:

Potable water requirements vary between Medical Centers and depends upon the number of persons expected to remain at the facility throughout the emergency. The requirements for potable water storage shall be estimated at 40 - 50 gallons/person/day. This calculation applies to one person at the facility 24 hours or 3 people working 8-hour shifts in one day.

The director of a mission critical facility, in consultation with the area emergency manager, shall provide an estimate of the total number of people expected to be on the site, including patients or residents, staff, family members (of patients, residents, and staff), visitors, and potential "refugees."

Background: The Department of Veterans Affairs commissioned a Pilot Study of Emergency Power and Water Supply During Natural Disasters and reviewed water supply requirements at 25 separate medical centers in hurricane prone areas. The study concluded that the minimum potable water requirements during contingency operations ranged from 40 - 50 gallons/person/day.

8.4.2.1.2 Industrial water:

Industrial water requirements, necessary to keep the cooling towers and therefore the chilled water system in operation, are approximately 40 gallons per day per ton of peak cooling capacity. Industrial water requirements include cooling tower and boiler make-up water. A peak summer and winter consumption shall be normalized over a 7 day period. The profile with the greatest 96 hour consumption shall be used to determine industrial water storage requirements.

Background: This requirement was derived from the same Pilot Study of Emergency Power and Water Supply During Natural Disasters. The study also concluded that it was necessary for the HVAC systems to be in continuous operation, not only to maintain comfortable temperatures for effective patient care, but also to dehumidify the buildings to lessen potentially destructive mold growth caused by loss of power and air conditioning in high humidity climates. Depending upon regional climatic conditions, this may not be the case in all geographic locations.

8.4.2.1.3 Fire Protection Water:

Provide a minimum volume of storage water to fight a single fire for the worst case scenario on the campus. Include both Mission Critical and Life Safety Protected facilities in determining the worst case fire scenario. **This quantity represents the volume required exclusively for fire protection and shall not be used to fulfill the requirements for any other water system design volume.** The volume of fire protection water shall not be adjusted lower than the calculated requirement. Mission critical facilities shall be sprinkler protected throughout.

Use Table 8.4.2.1 to determine minimum storage for non-sprinkler protected facilities and use Table 8.4.2.2 for sprinkler protected facilities in calculating the single worst case fire scenario.

Note: Installing fire sprinklers in an existing non-sprinkler protected building may be a more cost effective solution than increasing the amount of water storage.

Table 8.4.2.1 Non-Sprinkler Protected Facilities*

NFPA 13 Hazard	Favorable	Unfavorable	Duration (Sec 5.2)	Total (Gallons)
Light Hazard Patient Buildings, Offices, Quarters	1,250 gpm		60 min	75,000
Light Hazard Patient Buildings, Offices, Quarters		1,500 gpm	120 min	180,000
Ordinary Hazard Laboratory Buildings, Shops, Laundries	1,250 gpm		60 min	75,000
Ordinary Hazard Laboratory Buildings, Shops, Laundries		2,000 gpm	120 min	240,000
Extra Hazard – Warehouse	1,500 gpm		60 min	90,000
Extra Hazard – Warehouse		3,000 gpm	120 min	360,000

* See VA FPDM 6th Edition Section 5

Table 8.4.2.2 Sprinkler Protected Facilities

NFPA 13 Hazard	Storage Volume (gallons) ^d
Light Hazard	24,000 ^a
Ordinary Hazard	49,500 ^b
Extra Hazard	180,000 ^c

- Based on the following: {0.1 gpm/ft² over 1500 ft² plus 250 hose stream} for 60 minutes.
- Based on the following: {0.2 gpm/ft² over 1500 ft² plus 250 hose stream} for 90 minutes.
- Based on the following: {0.4 gpm/ft² over 2500 ft² plus 500 gpm hose stream} for 120 minutes. The default design demand is 0.4 gpm/ft² over 2500 ft². However, where the largest demand for the campus is known to be less, the lesser demand can be substituted provided that the hose stream allowance and duration remain 500 gpm and 120 minutes respectively.
- Note: Densities and areas are from NFPA 13, but the hose stream allowances and durations have been adjusted to address VA requirements.

Requirements for fire protection water storage are based on the assumption that there will be only one fire at a time. The calculations shall assume that the water supply from off-site public water provider(s) will not be available. The water supply from on-site water sources, such as groundwater wells, shall only be included in the calculations when it can be documented that the water source, pumping facilities, and conveyance system are designed and constructed to provide continued operation during the emergency event.

8.4.2.1.4 Wastewater retention:

Wastewater storage requirements shall be sized to accommodate sanitary sewer flows anticipated from the potable water system and are estimated to be 40 - 50 gal/day/person and based on the same assumptions as the potable water calculations. Use of expandable storage bladders is an acceptable alternative to permanent tanks.

Note: This requirement was derived from the same Pilot Study of Emergency Power and Water Supply During Natural Disasters assuming that municipal lift stations and plants would fail during a disaster, and that VA would not wish waste to be discharged into the surrounding neighborhood. If the Medical Center's waste drains by gravity to the treatment plant, or there is sufficient storage volume in the piping systems, then wastewater retention storage may be reduced.

8.4.2.1.5 Contaminated water:

Designated sites that are implementing VHA's mass-casualty decontamination program shall include provisions for a permanent or portable holding tank for water contaminated with hazardous material(s).

Background: On November 7, 2002, the President signed Public Law 107-287, Department of Veterans Affairs Emergency Preparedness Act of 2002, which established that VA must provide decontamination at VHA medical facilities. EPA published Chemical Safety Alert EPA 550-F-00-009 (July 2000) First Responders' Environmental Liability due to Mass Decontamination Runoff which provides guidance on the collection of wastewater from decontamination operations.

8.4.2.2 Water Level Monitoring:

Water level must be remotely monitored in accordance with NFPA 22 and NFPA 72 at a constantly attended location, preferably at the Engineering Control Center (ECC), boiler plant or other 24-hour manned location. In locales subject to freezing, water temperature of above-ground storage tanks must likewise be monitored at a constantly-attended location.

8.4.2.3 Generator fuel:

A peak summer and winter consumption profile shall be normalized over a seven day period. The profile with the greatest consumption shall be used to determine generator fuel storage requirements. Boiler and generator fuel storage may be combined as allowed by applicable codes and operational criteria.

8.4.2.4 Boiler fuel:

Facilities firing coal as the main fuel normally store a sufficient supply of fuel to meet the normal demands of continuous operation for a period of 15 January days. Facilities firing oil as the main fuel must maintain a supply of fuel sufficient to meet the normal demands of continuous operation for a period of 15 January days. Plants that generate less than 50 percent of their annual steam demand by natural gas for 2 consecutive years are to be considered as burning oil only. Facilities firing natural gas as the main fuel with oil or propane back-up normally maintain a sufficient supply of back-up fuel to meet the normal demands of continuous operations for a period of 10 January days. See VHA Directive 2008-062 Boiler Plant Operations.

8.4.3 Water Storage Emergency Connection

The water storage system shall include emergency connections to allow for a change in supply source or change in delivery points.

8.4.4 Water Treatment

Provide water treatment equipment to mitigate from environmental contaminants including but not limited to fungi, dust, debris, outside condensation, and corrosion.

8.4.5 Onsite Water Well

Where available and permitted, use an onsite water well as an alternate source for potable, industrial, and/or fire protection water. The water supply from on-site water wells shall only be included in the calculations when it can be documented that the water source, pumping facilities, conveyance system, and storage reservoirs are designed and constructed to provide continued operation during the emergency event and meet the peak water demand criteria listed in section 8.4.2. Water tanks will be required to allow a balanced flow through pipelines, maintain pressure in distribution system, and serve as a buffer between the source and treatment plant. Provide emergency power to all equipment.

8.4.6 Protection of Equipment

Protect all water and fuel storage, pumping, metering, and regulating equipment with screen walls or barriers that comply with section 6.1. For elevated water towers, fence is acceptable as a barrier. All tanks shall remain functional and accessible during emergencies.

Underground storage vaults shall be water tight and tanks secured to prevent buoyancy. Intakes and vents for vaults shall be located above grade, above the base flood level elevation, unobstructed, and in areas not subject to flooding. Secure underground storage tanks to prevent buoyancy. Provide electronic security system for access control, intrusion detection, and monitoring of the critical equipment in accordance with Chapter 10.

8.4.7 Electrical Power

All electrical equipment necessary to operate stored water and fuel systems shall be backed by the standby electrical system.

8.4.8 Existing Facility – Water and Fuel Storage

Existing sites containing mission critical facilities shall comply with the requirements of section 8.4.

9 BUILDING SYSTEMS

9.0 Scope, Purpose, and Goals

This chapter describes criteria for building mechanical building systems (fuels, steam, and chilled water), building plumbing systems (potable water, fire protection water, sanitary sewer, and medical and laboratory gases and vacuum systems), building water storage systems (potable and industrial water storage tanks, water wells, pumps, and water purification systems), building electrical power distribution systems, standby electrical systems, UPS systems, and building telecommunications systems (demarc room, main computer room, telecommunications rooms, WLAN system, portable radio system, satellite radiotelephone system, public address system, distributed antenna system, and VSAT data terminal system). The building systems shall be designed in accordance with the VA Design Manuals including the Electrical, HVAC, Plumbing, Fire Protection, and Sanitary Design Manuals; specifically, all requirements of the VA Fire Protection Design Manual (which covers all VA construction) and the OIT Design Guide (which covers all spaces under OIT's purview) remain in effect. In addition, building systems that are necessary to keep a mission critical facility in operation shall not be located in high risk areas.

9.0.1 Modularity

Component modularity of major mechanical, electrical, and telecommunications systems is an overarching physical security precept, which suggests that building systems be designed and constructed from interchangeable components. Modularity is also integral to the VA Hospital Building System Research Study Report (VAHBS or Red Book) and its Supplement, which describe integrated and modular design for new facilities. Building systems for mission critical facilities shall employ the principles of modularity outlined in the VAHBS. The primary objectives of VAHBS modularity are cost control, improved performance, adaptability, and the provision of a basis for building development and modification. The physical security benefit of VAHBS modularity is that it results in a facility composed of identical or nearly identical service modules, each of which contains standardized mechanical, electrical, and telecommunications components that allow for isolation of service modules, simplification of maintenance and repair, and a higher degree of system capability and integrity. Each service module is in one fire compartment, and a fire compartment may contain more than one service module. VAHBS modularity reduces complexity in detailing and construction, reduces compromises in maintenance, and enhances physical security and future expansion.

9.0.2 Security Considerations

Refer to Chapter 5, Chapter 10, and Appendix A, Security Door Opening Matrix, and Appendix B, Security System Application Matrix, for construction and security requirements for mechanical, electrical, and telecommunications spaces.

9.1 HVAC systems

9.1.1 Requirements

9.1.1.1 Equipment location: Locate major mechanical equipment above the ground floor, above grade, and in an area not subject to flooding.

9.1.1.2 Emergency connections: Include emergency connections for chilled water and steam services at or near the building entrance point, where it will be unobstructed and accessible, above grade, in an area not subject to flooding. Where looped systems enter the building at two points, the emergency connections need only be installed on one entry.

9.1.1.3 Security control center (SCC): In the SCC, provide a display-only terminal, which will display status and alarm conditions reported by the energy center, the building(s) environmental control system(s), medical gas and vacuum system alarms, standby and/or emergency generators, and other similar systems.

9.1.1.4 Entrances and lobbies: Maintain positive pressure in lobbies and entrance areas.

9.1.2 Intakes and Exhausts

9.1.2.1 Outdoor air intakes: All air intakes shall be located so that they are protected from external sources of contamination. Locate the intakes away from publicly accessible areas, minimize obstructions near the intakes that might conceal a device, and use intrusion alarm sensors to monitor the intake areas.

- Locate all outdoor air intakes a minimum of 50 feet (15 m) from areas where vehicles may be stopped with their engines running.
- Locate all outdoor air intakes a minimum of 30 feet (9 m) above finish grade or on roof away from the roof line.

9.1.2.2 Air intakes and exhausts: Design to minimize the blast over pressure admitted into critical spaces and to deny a direct line of sight from a vehicle threat located at the standoff distance to the critical infrastructure within. Refer to Chapter 6.

9.1.2.3 Hurricane areas: Louvers in areas prone to hurricanes or wind-debris hazards (in accordance with ASCE 7-10) shall be certified by the manufacturer to meet the following Florida Building Code tests: Uniform Static Air Pressure Test, Cyclic Wind Pressure Test, Large Missile Impact Test, and Wind Driven Rain Resistance Test.

9.1.3 Existing Facility – HVAC Systems

Existing facilities shall comply with sections 9.1.1.2 and 9.1.1.3.

- Impact and wind driven rain resistant louvers, hardened plenums, and structured baffles, as described in section 6.5.1, shall be installed when a major interior renovation or major equipment replacement is performed. Refer also to section 6.5.2.

9.2 Electrical Systems

9.2.1 Standby Electrical System

Generators are required to provide power for the entire mission critical facility load. See also Chapter 5 for functional area requirements. The standby electrical system consists of generators, switchgear, fuel storage, and distribution equipment necessary to provide standby power to the mission critical facility. The standby electrical system is not identical to the NFPA-required ESS, which supplies power to a specifically mandated set of health care facility loads. The standby electrical system is in addition to the ESS. Refer to Section 4.10 of the VA Electrical Design Manual for additional information.

It is permissible for the standby electrical system to provide power to the ESS when the standby electrical system meets the requirement of the NFPA 99, NFPA 110, and other applicable codes.

Per VA Directive 0055, medical centers are ideal candidates for implementation of cogeneration (combined heat and power) systems because both steam and electricity are required year-round. Cogeneration systems will be considered to be the system of choice for all new medical facilities. Documentation will be required for any deviation from this policy.

Note that the requirement for onsite fuel storage eliminates natural gas cogeneration engines from consideration. Diesel-fueled engines are required.

9.2.1.1 Standby generators: Generators shall be diesel compression engine type rated as Limited Running Time prime power. Generators should provide power at the highest practical voltage level, preferably the medium voltage utility service entrance voltage, and be paralleled into the normal power electrical system at a point as close as possible to the utility service entrance. Based on VA experience with mission critical facilities of various ages in various climates and under diverse operational circumstances, a conceptual load of 5 watts per building gross square foot is recommended as an initial calculation point. The designer is to develop a design based on actual project requirements and conditions, including utility demand data, operational considerations, projected load reductions or growth, and applicable codes and VA criteria.

9.2.1.2 Location: Generators, paralleling equipment, and associated fuel and electrical components for standby power systems and EES shall be located above grade and above the 100-year floodplain and within dedicated, environmentally-controlled structures or rooms. These structures or rooms and their external features, such as air intakes or exhausts, shall be in compliance with the Physical Security Design Manual. Standby power systems shall be located a minimum distance of 50 feet (15 m) or greater in all directions from high-risk areas.

9.2.1.3 Load shedding controls: Automatic controls shall selectively shed load from the standby power system upon failure of one or more standby generators to operate. The last loads to be shed shall be the “normal” sources for the Essential Electrical System automatic transfer switches.

9.2.1.4 Emergency connections: Include an exterior emergency quick connection and all associated equipment for the ESS at or near the location of the EES distribution equipment.

9.2.2 Uninterruptible Power Supply (UPS)

Provide UPS equipment for critical telecommunications and computer equipment. The telecommunications facilities include the entrance facility (*demarc*), main computer room, and telecommunications rooms. UPS equipment provides power during the time gap between loss of utility power and energization of the EES or standby electrical systems. UPS also provides power for an orderly shutdown of equipment in the event EES or standby electrical systems do not operate properly.

9.2.2.1 Modularity: Where multiple UPS are used, they shall be identically sized to allow for interchangeability.

9.2.2.2 Space for UPS: Provide required UPS floor space in rooms which require UPS-backed power.

9.2.2.3 Battery runtime: Size battery systems for a minimum of 20 minutes of full rated output. Individual project needs may dictate a longer runtime.

9.2.3 Existing Facility – Electrical Systems

9.2.3.1 Standby electrical system: Existing facilities in regions prone to hurricanes (in accordance with ASCE 7-10) and zones of Moderate-High or greater seismicity (refer to VA H-18-8) shall comply with section 9.2.1. Facilities outside these areas or zones are encouraged to comply with section 9.2.1.

9.2.3.1 UPS: Existing facilities shall comply with section 9.2.2.

9.3 Telecommunications Systems

Refer to Chapter 5 for functional area requirements.

9.3.1 Demarcation Room

The demarcation room (*demarc*) is where all telecommunications services from all service providers are delivered to the building and contains the separation points between utility-owned and VA-owned equipment and cabling.

9.3.1.1 Location: The demarc room shall be located above grade and above the 100-year floodplain and within a mission critical building envelope. The room shall not be located adjacent to the main computer room. The room shall be located at least 50 feet (15 m) from high-risk areas, shall not be located within 25 feet (7.62 m) of an outside wall or delivery area, and shall not be located directly below laboratories, kitchens, laundries, toilets, showers, or other areas where water service is provided.

9.3.1.2 HVAC: The demarc room shall be provided with generator-backed HVAC service.

9.3.1.3 Power: All equipment in the demarc room shall be powered from UPS equipment that will provide a minimum of 4 hours of service at full rated output. In addition, a risk analysis shall be performed to demonstrate the need for compliance

with NEC Article 708, Critical Operations Power Systems. Compliance with the provisions of NEC 708 may be required for the electrical systems serving the demarc room, including but not limited to upstream electrical distribution equipment.

9.3.1.4 Conduit pathways: Conduit pathways used to interconnect the demarc room and the main computer room shall be configured in a ring topology to provide two pathways between the two locations.

9.3.2 Main Computer Room

The main computer room contains all of the main telephone switching and data processing equipment for the mission critical facility.

9.3.2.1 Location: The main computer room shall be located above grade and above the 100-year floodplain and within a secure area of the building, on the ground floor or higher. The main computer room shall be located at least 50 feet (15 m) from high risk areas; shall not be located within 25 feet (7.62 m) of an outside wall or delivery area; shall not be located adjacent to the demarc room; and shall not be located directly below laboratories, kitchens, laundries, toilets, showers, or other areas where water service is provided.

9.3.2.2 HVAC: The main computer room shall be provided with generator-backed HVAC service.

9.3.2.3 Power: All equipment in the main computer room shall be powered from UPS equipment that will provide a minimum of 20 minutes of service at full rated output. In addition, a risk analysis shall be performed to demonstrate the need for compliance with NEC Article 708, Critical Operations Power Systems. Compliance with the provisions of NEC 708 may be required for the electrical systems serving the main computer room, including but not limited to upstream electrical distribution equipment.

9.3.2.4 Conduit pathways: Conduit pathways used to interconnect the demarc room and the main computer room shall be configured in a ring topology to provide two pathways between the two locations.

9.3.3 Telecommunications Rooms

Telecommunications rooms are located on all floors of the building and distribute telephone, data, and other telecommunications services to work spaces located throughout the building.

9.3.3.1 HVAC: Telecommunications distribution rooms shall be provided with generator-backed HVAC service.

9.3.3.2 Power: All equipment in the telecommunications rooms shall be powered from UPS equipment that will provide a minimum of 4 hours of service at full rated output. In addition, a risk analysis shall be performed to demonstrate the need for compliance with NEC Article 708, Critical Operations Power Systems. Compliance with the provisions of NEC 708 may be required for the electrical systems serving the telecommunications rooms, including but not limited to upstream electrical distribution equipment.

9.3.4 Wireless Local Area Network System

A wireless local area network (WLAN) data system facilitates rapid restoration of limited data communications services in the building after a catastrophic event. Provide a wireless data access system, or install infrastructure (cabling) placed for later system installation.

Provisions shall be made during the initial telecommunications system design and installation to implement a wireless data system throughout the building. These provisions are required whether a wireless data system will be initially installed or not. Specific design requirements will include placement of data access points, plans to interface with antenna distribution system, and equipment space and power requirements in telecommunications distribution rooms.

System design shall include provision for Power over Ethernet (PoE) to supply power to any individual access points.

Horizontal cabling used to connect Wireless Access Points (WAPs) shall be the same type as cable used for other building wireless access points.

WLAN access points distributed throughout the facility shall be secured to the ceiling or building in a way that requires a special tool for removal.

Data security on the WLAN shall be implemented using the most secure industry standard at the time the system is actually put in operation.

System design shall include the ability for the wireless data system to use the building distributed antenna system, where available, for distributing data signals.

9.3.5 Portable Radio System

Provide a portable radio system. The portable radio system provides two-way radio communications for security services and facilities management services both inside buildings and throughout the campus, where there are multiple buildings.

All fixed radio equipment shall be mounted according to manufacturer's recommendations and mounting provisions shall comply with applicable *seismic* requirements.

9.3.5.1 Location: Radio equipment may be located in a penthouse or one of the telecommunications rooms. The location must be coordinated with access to both the antenna equipment and the telecommunications rooms. Radio equipment shall not be located adjacent to the demarc or computer rooms and shall be located at least 50 feet (15 m) from high risk areas, shall not be located within 25 feet (7.62 m) of an outside wall or delivery area, and shall not be located directly below laboratories, kitchens, laundries, toilets, showers, or other areas where water service is provided.

9.3.5.2 HVAC: Rooms housing fixed radio equipment shall be provided with generator-backed HVAC service.

9.3.5.3 Power: Fixed radio equipment shall be powered from UPS equipment that will provide a minimum of 20 minutes of service at full rated output. In addition, a risk analysis shall be performed to demonstrate the need for compliance with NEC Article 708, Critical Operations Power Systems. Compliance with the provisions of NEC 708 may be required for the electrical systems serving the portable radio system.

9.3.6 Satellite Radiotelephone System

Provide a satellite radiotelephone system. The purpose of the satellite radiotelephone is to provide a very basic and limited telephone capability in the event internal and external phone systems failure. The satellite radiotelephone must be able to make local, long distance, and international telephone calls directly over a satellite connection without using any land facilities.

9.3.7 Public Address System

Provide public address (PA) systems in accordance with other VA design manuals, design guides, and specifications.

9.3.7.1 Location: All central PA equipment shall be located in the main computer room to facilitate interconnection with the telephone system.

9.3.7.2 Power: PA system equipment shall be powered from UPS equipment that will provide a minimum of 20 minutes of service at full rated output. In addition, a risk analysis shall be performed to demonstrate the need for compliance with NEC Article 708, Critical Operations Power Systems. Compliance with the provisions of NEC 708 may be required for the electrical systems serving the public address system.

9.3.7.3 Cabling: Comply with all cabling and installation practices associated with equipment intended for use in a critical care facility.

9.3.8 Distributed Antenna System

Provide a distributed antenna system in the facility. The distributed antenna system works in conjunction with the various radio systems in the building to improve portable radio system coverage in the building and provides the ability to use one common antenna system for multiple services. Services that may be supported include the portable radio system, public safety radio rebroadcast, cellular radio system rebroadcast, and support for WLAN data service.

9.3.8.1 Location: All distributed antenna system equipment shall be located in the telecommunications rooms.

9.3.8.2 Power: Distributed antenna system equipment shall be powered from UPS equipment that will provide a minimum of 20 minutes of service at full rated output. In addition, a risk analysis shall be performed to demonstrate the need for compliance with NEC Article 708, Critical Operations Power Systems. Compliance with the provisions of NEC 708 may be required for the electrical systems serving the distributed antenna system.

9.3.8.3 Cabling: Comply with all optical fiber, coaxial, and antenna system cabling and installation practices associated with cabling intended for use in a critical care facility.

9.3.9 Very Small Aperture Terminal Satellite Data Terminal

A Very Small Aperture Terminal (VSAT) data terminal acts as a backup data system and provides limited data capability if all ground based services were to fail. It provides a data capability that is not dependent on local service providers.

9.3.9.1 Location: VSAT equipment is roof-mounted and interfaces with data translation equipment located in the main computer room.

9.3.9.2 Power: VSAT equipment shall be powered from UPS equipment that will provide a minimum of 20 minutes of service at full rated output. In addition, a risk analysis shall be performed to demonstrate the need for compliance with NEC Article 708, Critical Operations Power Systems. Compliance with the provisions of NEC 708 may be required for the electrical systems serving the VSAT.

9.3.10 Existing Facility – Telecommunications Systems

Existing facilities shall comply with section 9.3.

9.4 Plumbing Systems

9.4.1 Medical Gases, Vacuum, and Oxygen Systems

Medical gases, vacuum, and oxygen systems shall be secured to prevent unauthorized tampering, contaminating, or cross connecting of systems. Provide emergency connection points for skid-mounted medical air and vacuum equipment and skid-mounted liquid oxygen tank with evaporator and regulators.

9.4.2 Existing Facility – Plumbing Systems

Existing facilities shall comply with section 9.4.

9.5 Fire Protection Systems

9.5.1 Fire Sprinkler Systems

Mission critical facilities shall be sprinkler protected throughout.

9.5.2 Fire Department Hose Connections

Fire department hose connections located on the exterior of a building shall be protected in such a manner as to limit access only to authorized personnel. Protection devices shall be approved by the Authority having Jurisdiction (AHJ) and local Fire Officials.

9.5.3 Existing Facility – Fire Protection Systems

Existing facilities shall meet the requirements of section 9.5.

10 SECURITY SYSTEMS

10.0 Scope, Purpose, and Goals

The requirements of Chapter 10 shall apply to all mission critical facilities, both new and existing. Existing facilities shall be required to meet the same requirements as new facilities. The physical security of mission critical facilities focuses both on protection and safety of people and physical assets, requiring protection of facility systems necessary to maintain operations prior to, during, and after a manmade or natural event.

This chapter addresses physical security standards associated with the selection, application, and performance of electronic security systems (ESS). The ESS includes the *Physical Access Control System (PACS)*; *Intrusion Detection System (IDS)*; *Video Assessment and Surveillance Systems (VASS)*; *Duress, Security Phones, and Intercom System (DSPI)*, commonly referred to as intercommunications system; and the *Detection and Screening System (DSS)*. The integration and monitoring of the ESS, system operation, and space requirements associated with the ESS subsystems are discussed in this section. *Security Control Center (SCC)* and *Security Equipment Room (SER)* functional requirements are provided in Chapter 5, while operational and system requirements are found within this chapter.

The ESS subsystems shall be designed and engineered by a qualified security specialist complying with the requirements in section 1.5.

10.0.1 Guidance on use of this Section and Appendices A and B

The requirements provided within this chapter and Appendices A and B shall be used collectively to provide an acceptable level of security for the subject facility and/or site.

10.0.2 Designers Resources

The security consultant shall comply with VA's latest construction specifications for electronic security systems, found on the VA TIL, and augmented by VA Policies and Directives. Additional sections shall be prepared by the designer as necessary to suit the project requirements.

10.1 Electronic Security Systems

There is a higher need for event correlation and awareness for mission critical facilities. Mission critical facilities shall report up to a regional monitoring center to provide system resiliency and failover. All systems are required to be networked for identity verification as required by Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standards 201 (FIPS-201) compliance. Each mission critical facility shall have its own dedicated connection to the Federal bridge and PACS server. All PACS shall comply with HSPD-12 and NIST 800-16 requirements. These requirements are established in the Master Construction Specifications.

Integrate all ESS into a common graphic user interface (GUI) to provide comprehensive situational awareness. This includes correlating alarm events with automated video call-up of associated video for remote assessment. Linkages between systems shall be logical in lieu of complex hardwired systems using inputs and outputs.

Larger mission critical or regional systems shall consider the use of physical security information management (PSIM) systems to combine large complex subsystems. PSIM systems also provide the ability to monitor multiple security subsystems from multiple manufacturers. Regional monitoring systems are a VA goal and are encouraged. See *Physical Security: Electronic Security Systems Manual, Final Draft 2008* concerning regional monitoring systems.

A central interface shall be provided for monitoring, reporting, and configuration of all electronic security subsystems. It shall provide correlated event monitoring and controls. The ESS shall allow the configuration of alarm monitoring, administrative, asset management, digital video management, intrusion detection, visitor enrollment, remote access level management, and integrated security workstations.

The ESS shall have the ability to compose, file, maintain, update, and print reports for either individuals or the system. Examples of systems reports include:

- Individual reports consisting of an employee's name, office location, phone number or direct extension, and normal hours of operation and shall provide a detail listing of the employee's daily events in relation to accessing points within a facility.
- System reports producing information on a daily/weekly/monthly basis for all events, alarms, and any other activity associated with a system user.

All ESS with system clocks shall be connected to a time synchronization clock to provide a coordinated time stamp. The time synchronization system shall be based on an internal VA utilized time clock or atomic sync.

The ESS shall be backed by the standby electrical system and UPS equipment. Refer to Chapter 9 for utility and building system requirements.

10.2 Physical Access Control System

The physical access control system (PACS) consists of all equipment and information required to verify, identity, and grant or deny access to individuals in accordance with HSPD-12. Equipment ranges from card readers and locks to the servers and databases required for identity verification and all components and communication in between. Mission critical facilities shall have a SCC for monitoring with failover to a regional monitoring center.

10.2.1 ESS Hardware

10.2.1.1 Data gathering panels shall be centrally located within a secure location that prevents panels from being damaged, tampered with, or accessed by unauthorized personnel. Field modules, such as reader modules, may be located on the secured side of a door in an enclosure that is locked or protected with a tamper switch.

10.2.1.2 Entry control devices include card readers and biometric verification stations. All entry control devices shall be FIPS 201 compliant and hardwired to the PACS data gathering panel. Biometric systems have limited application and shall only be utilized for secondary authentication into high security areas.

10.2.1.3 Electrified locks, such as, magnetic locks, strikes, and mortise locks, shall be selected based upon life-safety requirements, locking arrangements, and level of security. Utilize request-to-exit devices integrated in the electrified locksets in accordance with NFPA, IBC, and other applicable construction codes. Fail-safe-fail-secure, field selectable locks shall be used.

10.2.1.4 Optical turnstiles, where used in high-traffic access control points such as lobbies, require integrated barriers. Rotary turnstiles are discouraged due to life-safety concerns. Coordinate and accommodate life-safety when planning to use turnstiles.

10.2.1.5 Credentials and enrollment interface: with the development of the HSPD-12 based architecture, credentialing and badge issuance are separate from the PACS. Facility level enrollment station will be required; however, credentialing and badge issuance will be accommodated by a separate non-PACS system. The facility level enrollment station will allow the PIV badge holder to be programmed for facility level access permissions. Credential validations shall comply with OMD 11.11, FICAM, and NIST SP 800-116, and shall use PKI authentication method.

10.2.1.6 Locations: Refer to Appendix A, Security Door Opening Matrix, and Appendix B, Security System Application Matrix, for PACS system component locations.

10.3 Intrusion Detection System

The intrusion detection system (IDS) consists of all equipment and information required to detect and annunciate potential unauthorized entry into a protected space through an accessible and man-passable opening. An accessible opening as defined by NFPA 730 *Guideline for Premise Security* is within 18 feet (4 m) of exterior ground surface or within 18 feet (4 m) directly or diagonally opposite a window, structure, fire escape, or roof. A man-passable opening as defined by NFPA 730 is a clear cross section area of 96 square inches (619 cm²) or more with the smallest dimension exceeding 6 inches (15.2 cm). IDS sensors include motion detection, glass break, door contacts, and other detection devices. All IDS shall meet UL 639 Intrusion Detection Standard. Terminate all IDS sensors on the PACS data gathering panel. Provide an arm/disarm panel in protected spaces. Pharmacies have additional requirements; refer to VA 0730, Appendix B for these requirements.

10.3.1 Planning and Selection Criteria

IDS shall provide multiple levels or points of detection as far as possible from an asset to be protected. Determine the type of IDS sensor technology to use based upon the capability of the sensor and environmental factors.

Intrusion devices of different technologies (such as, motion detection, glass break, or magnetic contacts) shall be zoned separately. Intrusion devices of like technologies shall be wired together, not to exceed three devices, within the confines of clear physical barriers and not to exceed 50 feet (15 m). Devices in the same physical location providing the same purpose shall be programmed in alarm groups to support the intrusion zone concept.

10.3.2 Data Transmission System

Sensors and arm/disarm devices shall be hardwired and directly connected to the data gathering panel whenever feasible. Wireless alarms may be used only where the surrounding building construction and environment will not degrade the effective range of the alarm signal. Where a wireless IDS system is used it shall meet Federal Communication Commission (FCC) wireless transmission standards and VA requirements, including coordination with proper approving authority within VA.

10.3.3 Interior Sensors

10.3.3.1 Balanced magnetic switches (BMS) may be either recessed or surface mounted; the preferred method is to use a recess mounted switch to reduce the ability to defeat the system and improve aesthetics.

- When double doors or gates require protection, each door shall be fitted with a separate magnetic switch.
- Surface mounted switches shall be mounted on the protected side of the door.
- When protecting roll-up doors wider than 80 inches (2 m), BMS shall be mounted on both sides on the interior side of door.

10.3.3.2 Glass break sensors: Windows with security mesh screen do not require glass break sensors. Consider window construction to mitigate blast or ballistic hazards when selecting sensor technology. Laminated glass thicker than 0.25 inches (0.635 cm) does not require IDS. Glass break sensors shall not be used in the absence of PIRs or balanced magnetic switches.

10.3.3.4 Passive infrared sensors: Passive infrared sensor (PIR) shall meet the requirements of ANSI/SIA PIR-01, *Passive Infrared Motion Detector Standard - Features for Enhancing False Alarm Immunity*. A 360-degree field of view configuration shall be preferred for sensor monitoring purposes, but the final determination of configuration for field of view, which may be 360, 180, 90, 45 degrees or curtain, shall be determined from a field survey and mounting surface availability. Sensitivity of the sensor shall be adjustable to provide the necessary area of protection.

10.3.3.5 Vibration sensors: Boundary walls to be protected shall use vibration detection sensors mounted to the wall to assure detection of attempted penetration before the wall is breached. Vibration sensors shall be used in combination with BMS

for safes and vaults. Wall mounted shock/vibration sensors shall be provided with LEDs to indicate activation and shall be mounted to provide a clear view of the LED. Except for unusually small areas, smaller than 10 x 10 feet (3 x 3 meters), sensors zoned together shall not cover more than one wall.

10.3.3.6 Video motion detection does not provide sufficient probability of detection with reasonable nuisance alarm rates to be considered intrusion detection; however, video motion detection maybe used in areas where alternate sensor or more conventional detection methods are not appropriate. The nuisance alarm rate (NAR) shall be less than 5 percent.

10.3.4 Exterior Sensors

Exterior intrusion detection systems shall be planned for remote VA utility infrastructure lacking physical guard or police force presence. These areas are commonly water towers and water treatment facilities outside the VA established perimeter but may include other assets. Exterior sensors shall only be used for perimeter protection when the area to be protected is bordered by a fence or physical barrier. Exterior perimeter detection capability shall be applied to fenced areas around a site or building, loading docks, and outside storage areas or enclosures, using volumetric sensors in addition to BMS on access gates. Facilities that use a fence to define boundaries shall address the use and necessity of fence mounted sensors, microwave sensors, or photoelectric beams.

10.3.4.1 Microwave sensors, where required for security, shall use a multiple-beam configuration and only be used when there is a clear line of sight between a transmitter and receiver and where the ground is within the sensor operational specifications. Microwave sensors shall not be used near outdoor fluorescent lights.

10.3.4.2 Infrared Sensors, where required for security, shall be used in a multi-beam arrangement to create an invisible fence or corral around the *protected area*. These systems are affected by fog, rain, and snow and shall not be installed where local climatic conditions would cause interference.

10.3.4.4 Fence mounted sensors, where required for security, shall include tension wire, capacitance, electric vibration, and shock sensors. When using fence mounted sensors a BMS shall be installed at the pedestrian and vehicle access point gates.

10.3.4.5 Video motion detection does not provide sufficient probability of detection with reasonable nuisance alarm rates to be considered intrusion detection; however, video motion detection maybe used in areas where alternate sensor or more conventional detection methods are not appropriate. The security consultant shall ensure that NAR is acceptable; an acceptable maximum shall be less than 5 percent.

10.3.5 Design and Installation

To ensure proper operation, maximum detection capability, and minimize false alarms, IDS shall be installed in accordance with manufacture instructions, NFPA 731 *Standard for the Installation of Electronic Premises Security Systems* and UL 681 *Installation and Classification of Burglar and Holdup Alarm Systems*. All IDS shall be capable of continuous operation and monitoring through the use of UPS equipment and standby electrical system (see Chapter 9).

10.3.5.1 Locations: Protect all man-passable openings in a building perimeter with contacts. Protect all accessible openings as defined by NFPA 730 with appropriate sensors. Refer to Appendix A, Security Door Opening Matrix, and Appendix B, Security System Application Matrix, for IDS system component locations.

10.4 Video Assessment and Surveillance

This section addresses physical security standards for the two basic uses of a VASS: event assessment and general surveillance. This section describes the selection, application, and performance of the VASS, which includes cameras, monitors, controlling and recording equipment, and centralized management and operations of the system.

10.4.1 System Uses, Compatibility, and Integration

10.4.1.1 System uses: VASS shall be used to monitor building entrances, restricted areas, mission *critical asset* areas, and alarm conditions. VASS shall be used for surveillance and documentation of defined exterior areas, such as, site and roadway access points, parking lots, and building perimeter, and interior areas from a centralized SCC.

10.4.1.2 System compatibility: All components of the VASS shall be fully compatible and shall not require the addition of interface equipment or software upgrades to ensure a fully operational system.

10.4.1.3 System integration: The VASS shall be able to be fully integrated with other security subsystems.

10.4.2 Networked Versus Stand-alone

VASS shall be designed and engineered as either a networked or stand-alone system.

10.4.2.1 Networked VASS shall be utilized when multiple cameras, monitors, controllers, and recording devices are configured and makeup what is defined as a whole VASS. All components of the system shall be monitored and controlled in the SCC, using either a matrix switcher or a desktop computer. Alternate locations for monitoring cameras may be required in some circumstances.

10.4.2.2 Stand-alone VASS may be used for a single application and designated location use only and may compliment the PACS for a specific area. Fixed camera(s) shall be positioned in a manner to allow viewing of specific entry control point(s) through the use of a dedicated VASS monitor located in a common viewing area.

10.4.3 Cameras

The design, installation, and use of VASS cameras shall support the visual identification and surveillance of persons, vehicles, assets, incidents, and defined locations.

10.4.3.1 General requirements: All cameras shall meet the following requirements.

- Cameras shall conform to National Television System Committee (NTSC) formatting criteria.

- Cameras shall be color and auto-day/night feature to digitally switch from color to black and white at dusk and vice versa at dawn.
- Cameras shall be rated for continuous operation.
- Each camera function and activity shall be addressed within the system by a unique twenty character user defined name. The use of codes or mnemonics identifying the VASS action shall not be accepted.
- Cameras shall have built-in video motion detection that automatically monitors and processes activity information from each camera, based upon how the surveillance field-of-view is programmed.
- When the camera is used as part of a VASS computer network, a video encoder shall be used to convert the signal from the NTSC criteria to Moving Picture Experts Group (MPEG) format.
- All cameras shall be home run to a monitoring and recording device via controlling video equipment such as a matrix switcher or network server that is monitored from a designated SCC location. The use of wireless cameras are discourage for any long term application (more than 1 year period of use) and shall not be used for mission critical assets (see section 10.4.3.3 wireless camera use).

10.4.3.2 Fixed versus pan/tilt/zoom: VASS cameras may be either fixed or pan/tilt/zoom (P/T/Z).

- Fixed cameras shall be the primary means of surveillance to monitor designated access control and monitoring points.
- Fixed cameras shall be used to monitor interior building areas; P/T/Z cameras may be used to provide supplemental surveillance coverage of building interiors where necessary.
- P/T/Z cameras shall be used and deployed for all site perimeter and exterior building areas.

10.4.3.3 Hardwired versus wireless: VASS cameras classified as hardwired directly connect to a monitoring device using video signal imaging cable. A wireless VASS camera application is directly connected via a remote receiver that requires constant line-of-sight communications with the camera and the monitoring device.

- Hardwired or Internet protocol (IP) cameras shall be the preferred method of installation.
- Hardwired cameras shall be connected to the monitoring equipment with continuous wiring used as the media transmission system.
- Prior to selection of wireless cameras, consider the potential effects on the use of this technology, such as geographical area of coverage, environmental interference, effects on medical systems, and distance from the monitoring location.
- Wireless systems shall meet FCC requirements and be approved by VA wireless system approval authority during the design of the system.

10.4.3.4 Color versus black and white: All VASS cameras shall be color that allows for black and white applications.

- Cameras shall be able to switch between color and black and white through a programmable feature built into the camera (auto day/night feature).

- Color shall be the primary mode, automatically switching to black and white when light levels drop below normal specifications.

10.4.3.5 Camera lenses shall be used in a manner that provides maximum coverage of the area being monitored and shall meet the following requirements. Two types of lenses shall be used for both interior and exterior fixed cameras.

- Manual variable focus lenses shall be used in large areas monitored by the camera and shall allow for settings at any angle of field to maximize surveillance coverage.
- Auto iris fixed lenses shall be used in areas where a small specific point of reference is monitored.
- Specific lens size shall be determined using a field-of-view calculation provided by the manufacture.

10.4.3.6 Camera enclosures: All cameras and lenses shall be enclosed in tamper resistant housings.

- Both interior and exterior cameras shall be housed within a tamper-proof camera enclosure.
- Exterior camera enclosures shall be rated to protect against unique weather elements associated with the specific facility conditions and geographical area.

10.4.3.7 Camera installation, mounts, poles, and bases: All camera equipment shall be installed to ensure all components are fully compatible as a system. Adhere to guidance provided by the National Electrical Contractors Association Standard, NECA 303-2005, *Installing Closed-Circuit Television (CCTV) Systems*.

- Camera mounts shall be installed on approved mounting surfaces structured for weight, wind load, and extreme weather conditions.
- Camera mounts shall be installed in a manner that will not inhibit camera operation or field-of-view.
- Where a camera is mounted to a rooftop or within a parapet, ensure that the mount is designed and installed in a manner that the equipment can be swiveled inward for maintenance and upkeep purposes.
- All camera poles shall be constructed of metal with a concrete base and shall be installed and grounded in accordance with the NEC.
- Camera poles shall be weather resistant.
- Cameras and their mounts may share the same pole with lighting when the following conditions are met:
 - A hardened wire carrier system is installed inside the pole to separate the high voltage power cables for the lighting from the power and signal cables for the camera and mount.
 - The camera and mount are installed and positioned in a manner that the lighting will not deter from, cause blind spots or shadows, or interfere with the video picture and signal.
- All camera poles and mounts shall be installed in locations that will allow for optimum view of the area of coverage.

10.4.3.8 Power source: All VASS cameras and mounts shall be powered remotely by a UL listed power supply unit (PSU) as follows:

- The PSU shall have the ability to power at least four exterior cameras or eight interior cameras.
- A back-up with dedicated power feed from a security system power panel shall be provided to the camera and mount. A step down transformer shall also be installed at the camera location to ensure a proper operating voltage is provided to the camera and mount.
- The VASS shall be supported by UPS equipment and standby electrical system (see Chapter 9).

10.4.3.9 Lightning and surge protection: With the exception of fiber optic cables, all cables and conductors that act as control, communication, or signal lines shall include surge protection when extending beyond the building envelope.

10.4.3.10 Site coordination: Site and building exterior lighting shall be coordinated and installed in a manner that allows the VASS system to provide positive identification of a person, vehicle, incident, and location.

- Lighting shall not provide bright illumination behind the main field of camera view.
- Cameras shall be installed in a manner that no lighting will point directly at the camera lens causing blind spots and black outs.
- Provide routine maintenance of lighting systems and replacement of lighting fixtures that are necessary for operational integrity of the VASS system.
- VASS cameras shall be installed so that landscaping will not deter from the intended field of view.
 - Cameras shall not be mounted in trees, bushes, or any other natural landscape that will in the long term degrade the view or operation of the VASS system.
 - Cameras shall not be installed behind, next to, or on any natural or manmade object that will restrict the field of view, cause signal loss, or prevent the camera from being fully operational.
 - Perform routine landscape maintenance that is necessary for operational integrity of the VASS system.

10.4.4 Additional Components

10.4.4.1 Monitors shall be color and able to display analog, digital, and other images in either NTSC or MPEG format associated with the operation of the security management system (SMS).

10.4.4.2 Matrix switcher/network server (controlling equipment) shall be used to call up, operate, and program all cameras associated VASS components. Controlling equipment shall have the ability to operate the cameras locally and remotely. A matrix switcher or a network server shall be used as the VASS controller. The controlling equipment shall allow the transmission of live video, data, and audio over an existing Ethernet network or a dedicated security system network, requiring an IP address or Internet Explorer 5.5 or higher. The controlling equipment shall be able to perform as an analog-to-Ethernet "bridge," allowing for the control of matrices, multiplexers, and P/T/Z cameras.

10.4.4.3 Keyboards and joysticks shall provide direct operator interface with the controlling equipment to allow for call-up, operation of cameras and mounts, and programming of controlling equipment as well as cameras and monitors. Where a matrix switcher is used, ensure the keyboard is outfitted with a joystick to provide direct interface with VASS camera controls.

10.4.5 Controlling and Recording Equipment

All cameras on the VASS shall be recorded in real time using a digital video recorder (DVR), network video recorder (NVR), or a time lapse video recorder (VCR). The type of recording device shall be determined by the size and type of VASS designed and installed, as well as the extent to which the system is to be used. The following criteria shall be followed when choosing a VASS camera recording device.

10.4.5.1 DVR shall be used within the VASS for large or small VASS system set-ups. The DVR may be used in place of a time lapse VCR regardless of how the VASS is designed and installed. The DVR may be installed with the SMS or as part of a VASS network. The DVR shall be IP addressable. Programming, troubleshooting, and all general maintenance and upgrades to the DVR shall be done locally at the recording unit.

- The DVR shall have a built-in compact disc-recordable (CD-R) for downloading of the buffer to compact disc (CD) for back-up.
- The DVR buffer shall be cleared and all information transferred to CD when the buffer is at no greater than 60 percent of capacity.
- Compact disc (CD) shall be stored in a dry, cool, central location that is secure. Recordings shall be stored in accordance with VA Police directives.

10.4.5.2 NVR shall be used within the VASS for large or small VASS system set-ups. The NVR shall be used when the VASS is configured as part of the SMS only. Input to the NVR shall be considered when designing and installing all cameras that will be connected to the NVR.

- Ensure the proper signal converter is used to interface non- PoE cameras over to a Category Five (CAT-V) cable.
- The NVR shall provide for either direct download of data to a computer storage device or CD. All storage media shall be stored in a dry, cool, central location that is secure, and storage media shall be held as directed by the VA Police.

10. 4.6 Video Motion Detection

VASS cameras shall have built-in video motion detection capability that automatically monitors and processes information from each VASS camera. Cameras shall be programmed to automatically change viewing of an area of interest without human intervention and shall automatically record the activity until reset by the VASS operator.

10.4.6.1 Timing: This feature shall detect motion within the camera's field of view and provide the SCC monitors immediate automatic visual, remote alarms, and motion-artifacts as a result of detected motion.

10.4.6.2 Interface with IDS: The video motion detection shall be interfaced with the IDS to provide redundancy in the security alarm reporting system.

10.4.6.3 Other system interface: Cameras shall be designed to interface and respond to exterior and interior alarms, security phones/call-boxes, duress alarms, and intercoms upon activation.

10.4.7 Camera Locations

Refer to Appendix A, Security Door Opening Matrix, and Appendix B, Security System Application Matrix, for VASS component locations.

10.5 Duress, Security Phones, and Intercom System

The section addresses physical security criteria associated with the selection, application, and performance of the duress, security phones or emergency call-boxes, and intercom system (DSPI), also referred to as the intercommunications system.

10.5.1 System Elements and Features

The DSPI system is used to provide security intercommunications for access control, emergency assistance, and identification of locations where persons under duress request a security response. Refer to Appendix B, Security System Application Matrix, for locations where DSPI devices shall be used.

10.5.1.1 DSPI system compatibility: All components of the DSPI shall be fully compatible and shall not require the addition of interface equipment or software upgrades to ensure a fully operational system.

10.5.1.2 System integration: DSPI shall be fully integrated with other security subsystems.

10.5.1.3 Handicapped accessibility: DSPI systems shall be accessible to persons with disabilities.

10.5.1.4 Security intercoms: The main components of this security subsystem are the hardwired master intercom and remote intercom stations. Intercom devices shall be integrated with the VASS upon initiation and activation of a two-way conversation. Where wireless systems are used, repeaters shall be required. Where a wireless intercom system is used; it shall meet FCC wireless transmission standards and VA requirements, including coordination with proper approving authority within VA. Typical locations for security intercoms shall include:

- Access controlled entry points to a site, parking, and perimeter building areas.
- Gated access and service road entry points.
- Loading docks and shipping/receiving areas.
- Interior building access control points to restricted areas.

10.5.1.5 Intercom door release: Security intercom with remote door release capability shall be used for functional areas that require PACS. The security intercom system shall be integrated with electronic or magnetic remote door release allowing for remote communication and unlocking of doors from a reception desk or SCC master intercom station. The security intercoms for these areas shall have both an audio and built-in video capability. Video verification of person(s) requesting access at these points shall be required.

10.5.1.6 Intercom master station shall be capable of selectively calling and communicating with all intercom stations individually or system wide. Master stations shall have a “call in” switch to provide an audible and visual indication of incoming calls from remote stations. The master station shall include, but not be limited to, a handset, microphone/speaker, volume control, push-to-talk button, an incoming call/privacy indicator, and selectors to permit calling and communicating with each remote or other master stations.

10.5.1.7 Intercom substation shall be capable of calling into a pre-programmed single or group of master stations via the pressing of a button or voice activation. When a programmed master station is not available, the call shall automatically transfer to another master station.

10.5.1.8 Multi-intercom station shall have the ability to call or monitor multiple stations individually or as a public address system.

10.5.1.9 Single intercom station only calls or monitors one other intercom location or station at a time; intercoms are direct wired and do not require a master station.

10.5.1.10 Push-to-Talk (PTT) two-way communications is the typical type of intercom activation device, which requires a button be pressed in order to transmit conversation over the intercom.

10.5.1.11 Voice operated intercom switching (VOX) automatically switches audio direction based on the sound of a voice. The switch works when a sound is detected by the speaker/transmitter and no push-button is required to transmit a communication. These intercoms shall be used in interior or exterior areas; however, not in areas with high background noise, such as parking garages.

10.5.2 Security Phones or Emergency Call-Boxes

An emergency call-box or telephone system shall be used instead of intercoms for a multi-facility environment, a stand-alone facility with a parking structure, or a site with a requirement to transmit call station communications to another site. Emergency call-boxes shall be used in areas such as parking garages/lots, sidewalks, pathways of large campuses, and in isolated areas.

10.5.2.1 Push button hardwired: Emergency call-box systems shall be hardwired to a master station located and monitored at a central location, preferably the SCC. Pushing and releasing the emergency call-box call button shall initiate a call-in to a pre-programmed master station. Once the button is pushed, hands free operation shall occur.

10.5.2.2 Handset-telephone extension: Emergency call-boxes shall have the capability of using the existing VA PBX telephone system lines. The PBX shall direct calls to a pre-programmed extension that may be located at a receptionist desk, the SCC, or both. Lifting the handset shall automatically dial a preprogrammed monitoring station. The caller’s location shall be defined in the PBX system. A minimum of two numbers shall be programmed into the system, so that if the first number is busy or unavailable the second number will be polled. VA facility telephone systems and emergency call-boxes shall not use automatic voice dialers to 911 or the municipal police department.

10.5.2.3 Speaker-handset stations: Emergency call-box stations shall have the capability to automatically cut out the loudspeaker at the station when the phone handset is lifted, allowing conversations to occur through the handset rather than a speaker.

10.5.2.4 Scream alert option: Emergency call-boxes shall provide the option that a speaker phone becomes activated when a loud scream is heard. This system shall be limited to indoor applications, such as stairwells and elevators or pre-defined high-threat locations, where background noise will not cause false activation of these devices.

10.5.2.5 Integration with VASS cameras: Emergency call-boxes shall provide coverage with VASS when activated or have a built-in camera video surveillance capability that can be monitored from the SCC upon device activation. See section 10.4.

10.5.2.6 Remote control and monitoring: Emergency call-box master stations shall have the capability of monitoring and automatically polling each call-box, report incoming calls, identify locations, and keep records of all call events via software and integration with the SMS. The system shall provide auto-answer capability to allow VA Police to monitor and initiate calls. The master stations shall have the capability to remotely adjust speakerphone and microphone capabilities and reset the call-box activation from the central monitoring station.

10.5.2.7 Signaling devices: Emergency call-boxes shall provide visual recognition devices such as strobes or beacons, which will provide identification of the activated call-box.

10.5.2.8 Outdoor vs. indoor locations: All emergency call-boxes shall be installed on rigid structures, columns, walls, poles, and/or freestanding pedestals that are easily identifiable through unique markings, striping or paint, signage or lighting, and shall remain easily visible during low light conditions. VASS and call-boxes shall be integrated to provide automatic surveillance and priority monitoring of the caller's location.

- Emergency call-boxes in indoor locations shall be easily accessible to the public, clearly marked, and may be wall mounted.
- All emergency call-boxes shall be accessible to persons with disabilities.

10.5.3 Duress/Panic Alarms

Duress/panic alarms shall be provided at locations where there is considerable public contact in isolated and pre-identified high-risk areas, such as the lobby reception desk, patient service areas, nursing stations, and isolated offices and buildings where VA personnel work. Upon activation, a silent alarm signal shall be sent to a centralized monitoring location that shall be capable of continuous operations. Other requirements associated with activated alarms shall include all of the following.

- Alarms shall be continuously monitored by the SCC.
- Activated alarms shall be integrated with VASS coverage of the area.
- Alarms shall be mounted in such a manner as not to be observable and shall prevent unintentional operation and false alarms.

- At strategic locations use PACS keypads that are capable of activation by a code known only to the user to notify the central monitoring station that the person entering an area is under duress.

10.5.3.1 Switch/push button hardwired: The duress/panic alarm system shall be hardwired to a monitoring site or the SCC. Upon activation of the alarm both a visual and audible alarm will be activated in the SCC. The system shall identify the location of the alarm by phone extension and area description.

10.5.3.2 Wireless: Before selection and installation of a wireless system a survey shall be conducted to determine if a wireless application is feasible. Wireless systems shall use ultrasonic, infrared, and radio frequency waves to link duress/panic devices with distributed transmitters and receivers. Receivers shall be mounted throughout an area or building, as needed, and hardwired to a central monitoring console. Repeaters shall be used to ensure full coverage. All wireless systems shall conform to FCC and VA standards for wireless communications systems. Authorization from the VA AHJ shall be required prior to specification of wireless devices.

10.5.3.3 Switch/push button telephone extension: This system shall use an existing telephone line and PBX to transmit a duress alarm. On activation the PBX shall direct the signal with the caller's location defined to a pre-programmed extension located at the SCC. VA facility telephone systems and emergency call-boxes shall not use automatic voice dialers to 911 or the municipal police department.

10.5.3.4 Wireless-pendant devices: Wireless duress/panic devices (also known as personal panic alarm, identification duress alarm, or man-down alarm) may be considered as an option. When the panic button is pushed a wireless alarm signal is sent to the closest installed wireless sensing unit, which sends the signal on to a designated alarm monitoring location. Only wireless alarms that provide both geographical location and identification of the individual and have been tested in the operational area, especially in isolated areas impacted by structures, topology and other influencing factors, shall be used. The use of these devices shall be limited to personnel identified as holding high-risk positions, work in isolated areas, or travel to/from parking areas and buildings that are isolated, especially during hours of darkness. Where a wireless pendant devices is used, it shall meet FCC wireless transmission standards and VA requirements, including coordination with proper approving authority within VA. The devices shall meet the following requirements.

- Be convertible and have the capability to be worn on a lanyard around the neck, belt clip, or wristband.
- Include low battery indicators that notify the user and monitoring station of their use.
- Be equipped with a pull chain that activates the device shall an attempt be made to forcibly remove it from the person carrying it.
- Only be operational while on VA facility property.

10.5.3.5 Locators and repeaters: The duress/panic alarm devices shall be integrated with SCC and SMS software to provide identification and location of the user. Locators shall be required for wireless/pendant devices. Where a wireless locator and repeater systems are used, they shall meet FCC wireless transmission standards and VA

requirements, including coordination with proper approving authority within VA. Requirements for locators and repeaters shall be as follows.

- Locators shall be placed in strategic locations such as hallways, gathering rooms, parking lots and garages, walking trails, or any place where the location of a person in duress is required.
- For large VA campuses and outside applications, repeaters shall be used that provide true line-of-sight range. The number of repeaters required will depend on the performance of a site survey, capabilities, and coverage distances.

10.5.3.6 Automated dispatch: Duress/panic alarm devices shall automatically announce or provide alarm notification signals to on-site pagers worn by VA Police and other designated personnel, hand held portable radios, cell phones, and landline telephones.

10.5.3.7 Integration with VASS cameras and IDS: Duress alarm areas shall be covered by VASS cameras. Once the duress alarm has been activated the VASS shall monitor and record all events associated with the alarm. The IDS will provide monitoring of duress alarm. Refer section 10.3.

10.5.4 DSPI Locations

Refer to Appendix B, Security System Application Matrix, for DSPI system component locations.

10.6 Detection and Screening Systems

Used only where specific site conditions require this level of security, detection and screening systems (DSS) include: *X-ray screening* machines, walk-through metal detectors (WTMD), hand-held metal detectors (HHMD), and desktop and hand-held trace/particle detectors (also called sniffers and *itemizers*). The use of DSS equipment may be provided as an optional means for screening persons, items, and materials that may possess or contain weapons, contraband, or hazardous substances prior to authorizing entry or delivery into a facility. Use of DSS equipment may be considered during periods of elevated credible threat from the National Terrorism Advisory System (NTAS) (formerly the Homeland Security Alert System (HSAS)). Each facility shall be addressed on a case-by-case basis concerning the use of DSS.

At a minimum, provide power and communications rough-ins for future installation of DSS equipment in the screening vestibule.

10.6.1 System Elements and Features

DSS are used for the pre-screening of persons, packages, and personal items for detection of contraband, such as, weapons, drugs, explosives, and other potential threatening items or materials, prior to authorizing building entry or delivery. Refer to Appendix B, Security System Application Matrix, for optional locations where DSS may be utilized.

10.6.1.1 DSS system compatibility: All components of the DSS shall be fully compatible and shall not require the addition of either software or hardware interface equipment.

10.6.1.2 System integration: The DSS shall be fully integrated with other security subsystems.

11 REFERENCES

This section lists applicable codes and regulations, standards, design guidelines, and resources.

The Facility Guidelines Institute

- Guidelines for Design and Construction of Health Care Facilities, 2010

American National Standards Institute (ANSI)

- ANSI/ASME B20.1-2009, Safety Standards for Conveyors and Related Equipment
- ANSI/SIA/CSAA SIA AC-01-1996, Access Control: Wiegand Card Reader Interface Standard
- ANSI/SIA/CSAA SIA AC-03-2000, Access Control: Badging Techniques
- ANSI/SIA/CSAA SIA AG-01-2000, Architectural Graphics—C AD Symbols Standard
- ANSI/SIA/CSAA SIA AV-01-1997, Two Way Voice Command Set Standard
- ANSI/SIA/CSAA STA1, Standard Documents
- ANSI/SIA/CSAA S3.2-2009, Method for Measuring the Intelligibility of Speech over Communications Systems
- ANSI/SIA PIR-01-2000, PIR Detector Standards
- ANSI/SIA/CSAA CP-01-2000, Control Panel: False Alarm Reduction Features Standard

American Society of Civil Engineers (ASCE)

- ASCE/SEI 7-10, Minimum Design Loads of Buildings and Other Structures

American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE)

American Society of Mechanical Engineers (ASME)

- ASME B20.1-2009, Safety Standard for Conveyors and Related Equipment

American Society for Testing and Materials (ASTM)

- ASTM C 1238-97(2003), Standard Guide for Installation of Walk-Through Metal Detectors
- ASTM F 1233-08, Standard Test Method for Security Glazing Materials and Systems
- ASTM F 476-84(2002), Standard Test Methods for Security of Swinging Door Assemblies
- ASTM F 567-11, Standard Practice for Installation of Chain-Link Fence
- ASTM F 588-07, Standard Test Methods for Measuring the Forced Entry Resistance of Window Assemblies, Excluding Glazing Impact

- ASTM F792-08, Standard Practice for Evaluating the Imaging Performance of Security X-Ray Systems
- ASTM F 842-04, Standard Test Methods for Measuring the Forced Entry Resistance of Sliding Door Assemblies, Excluding Glazing Impact
- ASTM F 883-09, Standard Performance Specification for Padlocks
- ASTM F2656-07, Standard Test Method for Vehicle Crash Testing of Perimeter Barriers

Architectural and Transportation Barriers Compliance Board (Access Board)

- Uniform Federal Accessibility Standards, 1984

Centers for Disease Control and Prevention (CDC)

- CDC list of high risk agents and material at <http://www.cdc.gov/>
- CDC-NIH Biosafety in Microbiological Laboratories

Code of Federal Regulations (CFR)

- 7 Code of Federal Regulations 331 and 9 Code of Federal Regulations 121: Agricultural Bioterrorism Protection Act of 2002; Possession, Use, and Transfer of Biological Agents and Toxins; Final Rule, March 18, 2005
- 14 CFR 108.17 and 129.26: Use of X-Ray Systems
- 21 CFR 1020.40: Cabinet X-Ray Systems
- 28 CFR Part 36-90: ADA Standards for Accessible Design
- 29 CFR 1910: Occupational Safety and Health Standards
- 36 CFR 1236.1236: Management of Vital Records, July 1, 1998
- 41 CFR 101-20.103-4: Occupant Emergency Program, July 1, 1998
- 42 CFR 72 & 73: Possession, Use, and Transfer of Select Agents and Toxins; Final Rule, March 18, 2005

Department of Defense (DoD)

- Unified Facilities Criteria (UFC) DoD Minimum Antiterrorism Standards for Buildings, UFC 4-010-01-22, January 2007 (Unrestricted)
- DoD Minimum Antiterrorism Stand-off Distances for Buildings, UFC 4-010-02-19, January 2007 (For Official Use Only)
- Design of Buildings to Resist Progressive Collapse, UFC 4-023-03-27, January 2010 (Unrestricted)
- Single Degree of Freedom Structural Response Limits for Antiterrorism Design, U.S. Army Corps of Engineers Protective Design Center (PDC) Technical Report, PDC-TR-06-08, Revision 1-07, January 2008 (Unrestricted)

**Department of Homeland Security (DHS)
Federal Emergency Management Agency (FEMA)**

- FEMA 426 Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings—Risk Management Series, December 2003
- FEMA 452 A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings—Risk Management Series, January 2005
- Homeland Security Presidential Directive (HSPD) 7: Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003
- Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors

**Department of Justice (DOJ)
Drug Enforcement Administration (DEA)**

- Drug Enforcement Administration, Schedule II-V Drug Security: <http://www.deadiversion.usdoj.gov/21cfr/cfr/2108cfrt.htm>

Department of State (DOS)

- SD-STD-01.01, Revision G, U.S. Department of State, Certification Standard Forced Entry and Ballistic Resistance of Structural Systems, April 1993
- SD-STD-02.01, Revision A, U.S. Department of State, Test Method for Vehicle Crash Testing of Perimeter Vehicle Barriers and Gates, March 2003

Department of Veterans Affairs (VA)

- NCA Design & Construction Criteria, <http://www.cfm.va.gov/til/nca.asp>
- VA Architectural Standard Details, Department of Veterans Affairs, Veterans Health Administration, Office of Construction and Facilities Management, Standard CAD Details Index, <http://www.cfm.va.gov/til/sDetail.asp>
- VA Design Manuals: Automatic Transport Systems, March 2011, <http://www.cfm.va.gov/dManual.asp>
- VA Design Manuals: Interior Design, May 2008, <http://www.cfm.va.gov/dManual.asp>
- VA Electrical Design Manual, April 2009, <http://www.cfm.va.gov/dManual.asp>
- VA Office of Information and Technology Design Guide, February 2011, <http://www.cfm.va.gov/dGuide.asp>
- VA Handbook 0320, Comprehensive Emergency Management Program, March 24, 2005, <http://www.va.gov/vapubs/>
- VHA Directive 0320, Comprehensive Emergency Management Program (CEMP), July 5, 2007, <http://www.va.gov/vapubs/>
- VA Handbook 0730/2, Security and Law Enforcement, 2000, <http://www.va.gov/vapubs/>
- VA Handbook 0730/2, Appendix B, Incremental Update, 2010, <http://www.va.gov/vapubs/>

- VA Handbook 7610, Space Planning Criteria, Undated, <http://www.va.gov/vapubs/>
- VA Handbook 1200.6, Control of Hazardous Agents in VA Research Laboratories, October 21, 2005, <http://www.va.gov/vapubs/>
- VA Handbook 1200.8, Safety of Personnel Engaged in Research, June 7, 2002, <http://www.va.gov/vapubs/>
- VHA Handbooks 1200.8, 1200.6; Memo dated 2007–BSL Research Lab Physical Security Inspections, <http://www.va.gov/vapubs/>
- VA Program Guide PG-18-3, VHA—Design and Construction Procedures, September 2010, <http://www.cfm.va.gov/til/cPro.asp>
- VA Program Guide PG-18-10, Architectural Design Manual, April 2011, <http://www.cfm.va.gov/dManual.asp>
- VA Program Guide PG-18-14, Room Finishes, Door and Hardware Schedule, March 2010
- VA Design Manuals: Physical Security: Electronic Security Systems Manual, Final Draft 2008, <http://www.cfm.va.gov/dManual.asp>
- VA Parking Design Guide, <http://www.cfm.va.gov/dGuide.asp>
- VA Seismic Design Requirements H-18-8, February 2011, <http://www.cfm.va.gov/TIL/seismic.asp>
- VHA Directive 2006-007, Ensuring the Security and Availability of Potable Water at VHA Facilities, <http://www.va.gov/vapubs/>
- VHA Directive 2008-062, Boiler Plant Operations, <http://www.va.gov/vapubs/>
- VHA Directive 2010-016, Inspection of All-Hazard Emergency Caches by the Emergency Management Strategic Health Care Group, <http://www.va.gov/vapubs/>
- VHA Directive 2008-001, All-Hazards Emergency Caches, <http://www.va.gov/vapubs/>

Florida Department of Community Affairs

- Florida Building Code, www.floridabuilding.org

General Services Administration (GSA)

- Interagency Security Criteria (ISC) for New Federal Office Buildings and Major Modernization Projects, September 29, 2004 (For Official Use Only)
- Interagency Security Criteria (ISC) Security Standards for Leased Space, September 29, 2004 (For Official Use Only)
- GSA Rated Storage Containers, <http://www.gsa.gov/Portal/gsa/ep/programView.do?pageTypeId=8207&oid=9760&programPage=%2Fep%2Fprogram%2FgsaDocument.jsp&programId=10598&channelId=-14005>

Government Accountability Office (GAO)

- GAO 03-8 Report of Federal Building Security

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE C62.41: Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits
- IEEE C95.1: Standards for Safety Levels with Respect to Human Exposure in Radio Frequency Electromagnetic Fields

International Code Council (ICC)

- International Building Codes, International Code Council

International Organization for Standardization (ISO)

- ISO 7816-1 (2011): Identification Cards – Integrated Circuit Cards – Part 1: Cards with Contacts - Physical Characteristics
- ISO 7816-2 (2007): Identification Cards – Integrated Circuit Cards – Part 2: Cards with Contacts - Dimensions and Location of the Contacts
- ISO 7816-3 (2006): Identification Cards – Integrated Circuit Cards – Part 3: Cards with Contacts - Electrical Interface and Transmission Protocols
- ISO 7816-4 (2005): Identification Cards – Integrated Circuit Cards – Part 4: Organization, Security and Command for Interchange
- ISO 14443 (2008): Identification Cards – Contactless Integrated Circuit Cards - Proximity Cards - Part 1: Physical Characteristics
- ISO 15693 (2009): Identification Cards Contactless Integrated Circuit Cards - Vicinity Cards – Part 3: Anticollision and Transmission Protocol

National Electrical Contractors Association (NECA)

- NECA 303-2005, Installing Closed-Circuit Television (CCTV) Systems

National Electrical Manufacturers Association (NEMA)

- NEMA 250-2008, Enclosures for Electrical Equipment

National Fire Protection Association (NFPA)

- NFPA 1: Fire Code 2012
- NFPA 70: National Electrical Code, 2011
- NFPA 75: Standard for the Protection of Information Technology Equipment, 2013
- NFPA 99: Standard for Health Care Facilities, 2012
- NFPA 101: Life Safety Code, 2012
- NFPA 110: Standard for Emergency and Standby Power Systems, 2013
- NFPA 730: Guide for Premises Security, 2011
- NFPA 731: Standard for the Installation of Electronic Premises Security Systems, 2011

- *Extreme Event Mitigation in Buildings: Analysis and Design*, NFPA, January 2006

National Institute of Justice (NIJ)

- NIJ levels: National Institute of Justice, U.S. Department of Justice, Ballistic Resistant Protective Material, NIJ Standard 0108.01-1985, Ballistic Resistant Protective Materials
- NIJ Standard 0601.02-2003: Walk Through Metal Detectors for use in Concealed Weapon and Contraband Detection

National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS)

- FIPS Pub 201-1, March 2006: Personal Identification Verification for Federal Employees and Contractors
- IR 6887 V2.1, July 2003: Government Smart Card Interoperability Specification (GSC-IS)
- Special Pub 800-96, PIV Card Reader Interoperability Guidelines, September 2006
- Special Publication 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), November 2008

National Institutes of Health (NIH)

- NIH Design Policy and Guidelines

Occupational Safety and Health Administration (OSHA)

- OSHA 29, CFR 1926N.555, Conveyor Belt Safety Standards

Underwriters Laboratories (UL)

- UL 50 Standards for Enclosures for Electrical Equipment, Non-Environmental Considerations
- UL 187 Standard for X-Ray Equipment
- UL 294 Standard for Access Control System Units
- UL 305 Standard for Panic Hardware
- UL 444 Communications Cables
- UL 497C Standard for Protectors for Coaxial Communications Circuits
- UL 603 Standard for Power Supplies for Use with Burglar-Alarm Systems
- UL 609 Standard for Local Burglar Alarm Units and Systems
- UL 636 Standard for Holdup Alarm Units and Systems
- UL 639 Standard for Intrusion-Detection Units
- UL 752 Standard for Bullet-Resisting Equipment
- UL 827 Central Station Alarm Services
- UL 969 Standard for Marking and Labeling Systems
- UL 1481 Standard for Safety for Power Supplies for Fire-Protective Signaling Systems
- UL 1981 Central Station Automation Systems

- UL 2058 High-Security Electronic Locks

U.S. Postal Service (USPS)

- Publication 166, Guide to Mail Center Security, March 2008

The Joint Commission (TJC)

- TJC Environment of Care Security Standards: <http://www.jointcommission.org/Standards/>

The White House

- Homeland Security Presidential Directive (HSPD) 7 Homeland Security Presidential Directive, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003
- Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors, 2004
- Homeland Security Presidential Directive (HSPD) 20, National Continuity Policy, 2007
- Executive Order 12472: Assignment of National Security and Emergency Preparedness Telecommunications Functions, April 3, 1984 (amended by EO 13286 of February 28, 2003 and changes made by EO 13407 June 26, 2006)
- Presidential Decision Directive (PPD) 62: Protection Against Unconventional Threats to the Homeland and Americans Overseas, May 22, 1998
- Presidential Decision Directive (PPD) 67: Enduring Constitutional Government and Continuity of Government Operations, October 21, 1999 (Superseded by HSPD-7)